Blockchain Security Alliance

BEOSIN Blockchain Security

SUSS NiFT Node for Inclusive Fintech

LegalDAO

Footprint Analytics

SHELLBOXES

Biteye

SECURING BLOCKCHAIN ECOSYSTEM

H1 2023

Global Web3 Security Report, AML Analysis & Crypto Regulatory Landscape

CONTENTS

Preface

With the continuous acceleration of the global digitalization process, blockchain, as an emerging decentralized trading method, is gradually becoming one of the core infrastructures of the digital economy. However, with the continuous expansion of blockchain application scenarios, the security risks users face are gradually increasing. Thus, understanding the security situation of Web3 and the regulatory policies of the crypto industry has become one of the necessary methods to ensure the security and stability of blockchains. This research report focuses on the global blockchain security situation in the first half of 2023, hot spots in Web3 and key regulatory policies of the crypto industry, and conducts an in-depth analysis and summary, aiming to provide readers with valuable reference and inspiration to help blockchain security grow healthily.

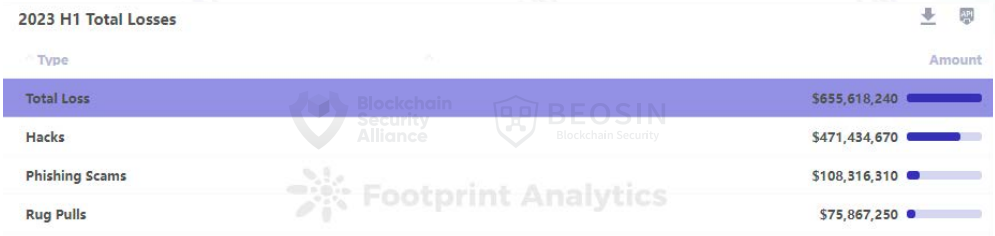
I.
H1 2023 Global Web3 Security Statistics & AML Analysis

This chapter was written by Mario & Donny from Beosin Research Team

Data source (As of June 25):
https://www.footprint.network/@Beosin/Footprint-Beosin-H1-2023-Report

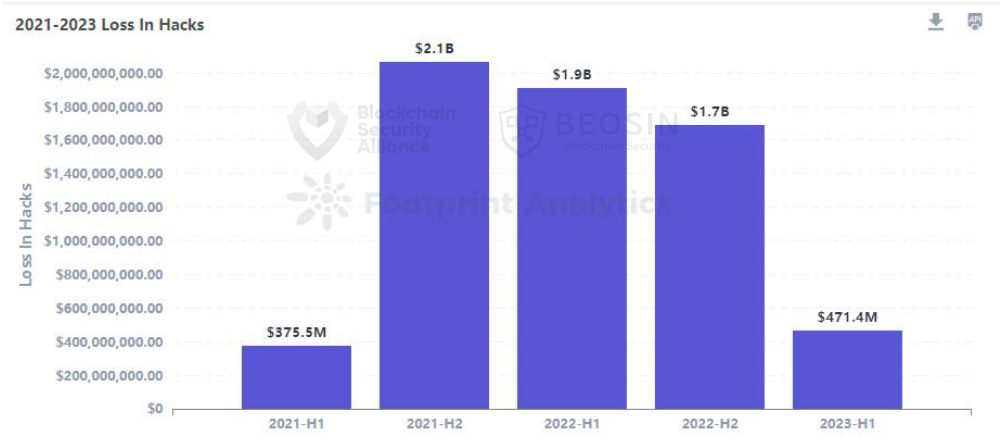
1. H1 2023 Web3 Security Overview

According to statistics from Beosin EagleEye platform, **the total losses from hacks, phishing scams, and rug pulls in Web3 reached $655.61 million in the first half of 2023.** Among them, **108 attacks** resulted in a total loss of approximately **$471.43 million. Phishing scams** accounted for a total loss of approximately **$108 million**, and there were 110 rug pulls with a total loss of approximately **$75.87 million.**



2023 H1 Total Losses

The total loss from hacks in Web3 has significantly decreased compared to last year. In H1 2022, the total loss from attacks was approximately $1.91 billion, and in H2 2022, it was about $1.69 billion, while in H1 2023, this value dropped to $471 million.



2021-2023 Loss In Hacks

In terms of project types, DeFi remains the most frequent target and the type with the highest losses. The total loss from 85 DeFi security incidents reached $292 million, accounting for 62% of the total losses.

In terms of blockchain platform types, **75.6% of the loss amount came from Ethereum,** totaling approximately $356 million, ranking first among all blockchain platforms.

In terms of attack types (classified according to root causes), the most frequent and financially damaging attack type was contract vulnerability exploits. **Sixty incidents of contract vulnerabilities resulted in a loss of $264 million, accounting for 56% of the total losses.**

In terms of fund flows, **approximately $215 million of stolen assets were recovered,** accounting for 45.5% of all stolen assets. Additionally, **approximately $113 million were transferred to Tornado Cash and other mixers.**

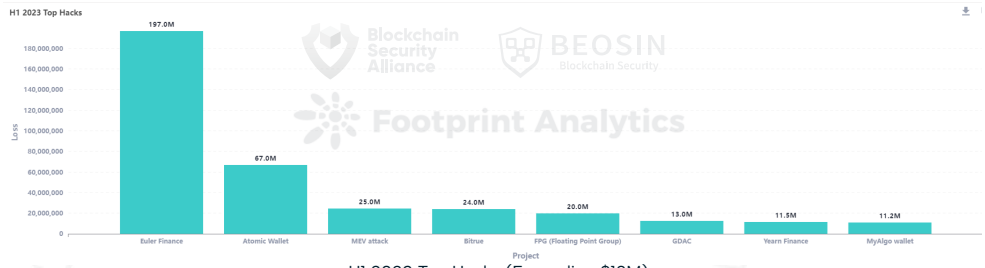
In terms of audit status, **approximately 49% of the attacked projects had not undergone an audit.**

In contrast to the decreasing trend in hackers compared to 2022, **phishing scams and rug pull events** were more frequent in the first half of 2023. According to incomplete statistics, **the total amount involved in these two types of events reached at least $184 million.** The lower barrier to entry for phishing scams, such as the sale of malicious toolkits by some wallet drainers where buyers can share profits with them after profiting, has led to a significant increase in phishing scams in the first half of 2023, becoming a major threat to the security of Web3 users.

2. Overview of Hacks

108 attacks resulting in $471.43 million in losses

In the first half of 2023, Beosin EagleEye monitored **108 major attacks in the Web3 space, with a total loss of approximately $471 million.** There was one security incident with loss exceeding $100 million, 7 incidents with losses ranging from $10 million to $100 million, and 23 incidents with losses ranging from $1 million to $10 million.



H1 2023 Top Hacks (Exceeding $10M)

Attacks with losses exceeding $10M (in descending order):

- Euler Finance - $197 million

On March 13, the DeFi protocol Euler Finance was attacked for $197 million. On April 4, Euler Labs announced on Twitter that the attacker had returned all stolen funds after successful negotiations.

- Atomic Wallet - $67 million

On June 3, several Atomic Wallet users reported on social media that their wallet funds had been stolen, with estimated losses of at least $67 million. The stolen funds were then laundered by the hackers through the Sinbad mixer, and the cause of the attack is still under investigation.

- MEV attack - $25 million

On April 3, several MEV robots were the victims of malicious sandwich attacks, resulting in a total loss of approximately $25 million.

- Bitrue - $24 million

On April 14th, cryptocurrency exchange Bitrue's hot wallet was hacked, leading to a loss of $24 million.

- FPG - $20 million

On June 11, cryptocurrency brokerage Floating Point Group (FPG) was attacked, resulting in a loss of approximately $20 million.

- GDAC - $13 million

On April 9, South Korean cryptocurrency exchange GDAC was targeted in a hack that resulted in a loss of nearly $13 million.

- Yearn Finance - $11.5 million

On April 13, Yearn Finance's YUSDT contract was hacked, resulting in a profit of over $10 million for the attacker.

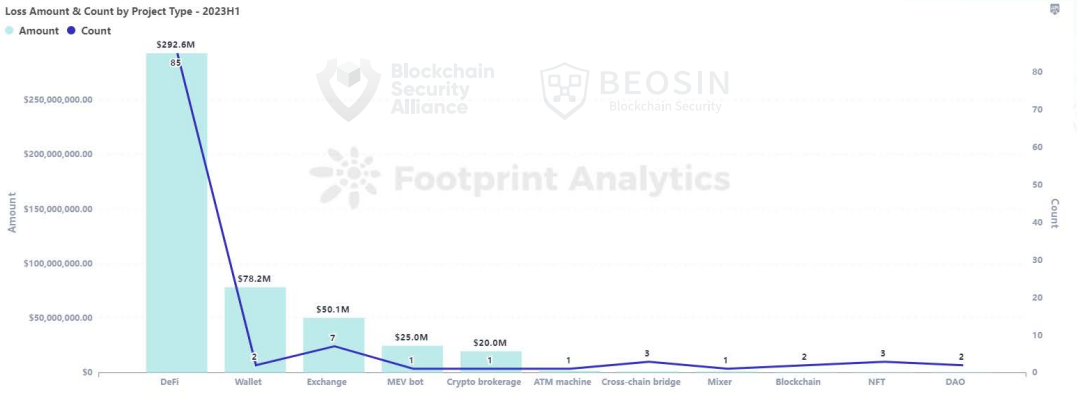
- MyAlgo Wallet - $11.2 million

In February, MyAlgo Wallet suffered a man-in-the-middle attack resulting in a loss of $11.2 million.

3. Types of Attacked Projects

$292 million lost in 85 DeFi security incidents

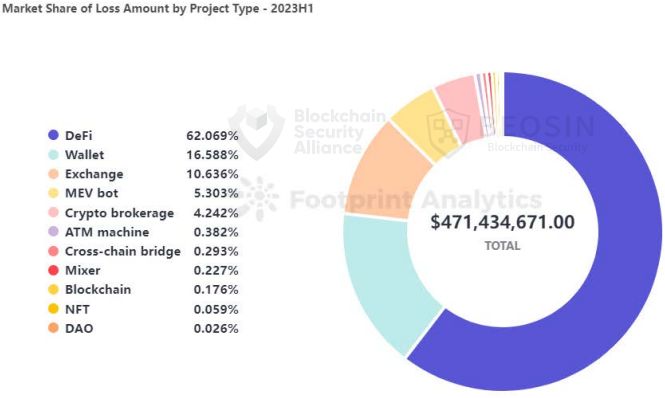
In the first half of 2023, a total of 85 security incidents occurred in the DeFi sector, accounting for 78.7% of the total number of attacks. The total loss in DeFi reached $292 million, representing 62% of the total loss. **DeFi projects experienced the highest frequency of attacks and the highest amount of losses compared to other project types.**



Loss Amount by Project Type

Out of the 85 DeFi security incidents, 51 incidents originated from contract vulnerabilities, resulting in a loss of $249 million, accounting for 85% of the total DeFi losses.

Wallet attacks caused approximately $78.2 million in losses, ranking as the second highest among all project types. The Atomic Wallet attack alone resulted in a loss of at least $67 million, while the MyAlgo wallet attack caused a loss of $11.2 million.



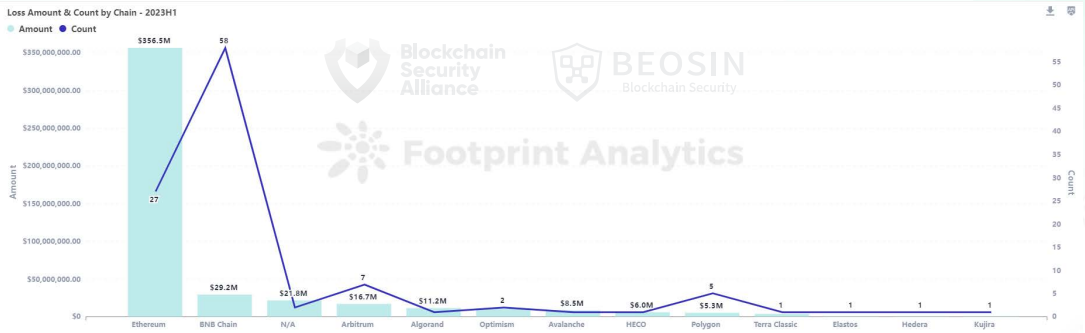
Loss Amount by Project Type (%)

The third-ranked project type in terms of losses is exchanges, with approximately $50.14 million in losses. Exchange attacks maintained a trend of frequent attacks, as seen in the ranking of losses throughout the entire year of 2022.

Cross-chain bridge projects ranked first in terms of losses in 2022 ($1.89 billion), but in the first half of 2023, the losses significantly decreased to $1.38 million.

4. Loss by Chain

75.6% of the loss amount was on Ethereum



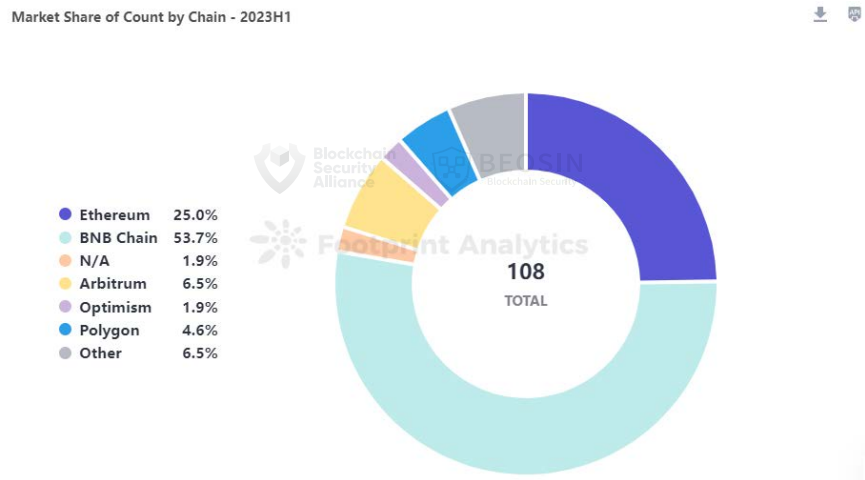
Loss Amount by Chain

In the first half of 2023, a total of 27 major attacks occurred on Ethereum, resulting in losses of approximately $356 million. Around 75.6% of the amount lost comes from Ethereum, ranking first among all chains.

BNB Chain witnessed the highest number of attacks, reaching 58 cases, which accounted for 53.7% of all security incidents. Out of the 58 attacks on BNB Chain, 40 of the targeted projects had not undergone any form of auditing.

A total of 7 attacks on Arbitrum have caused approximately $16.71 million in losses. Losses and the number of incidents have increased compared to 2022, where Arbitrum had only experienced two major security incidents throughout the entire year.

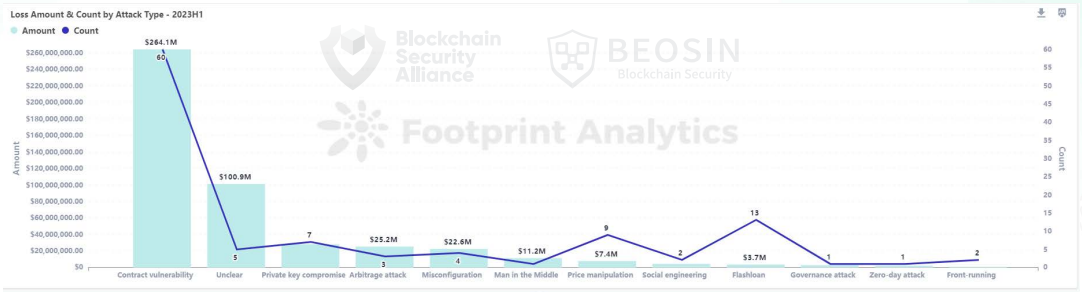
In 2022, Solana ranked third in terms of loss amount among all public blockchains. However, no major attacks were detected on Solana in the first half of 2023.



Count by Chain (%)

5. Loss by Attack Type

Contract vulnerability exploits saw the most frequency and the highest loss amount



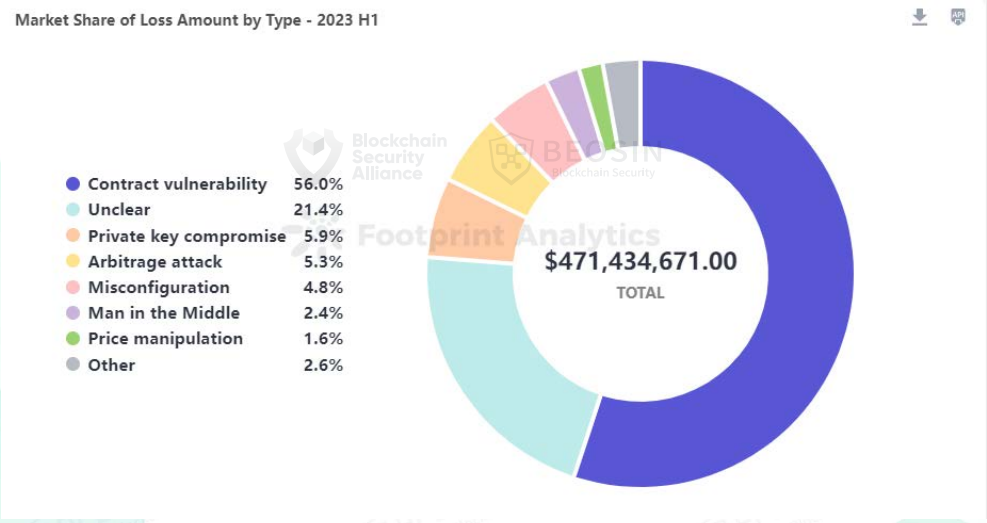
Loss Amount by Attack Type

**Note: When multiple attack techniques are present, classification is based on the root cause. Attacks with insufficient information or undisclosed reasons are classified as "Unclear."*

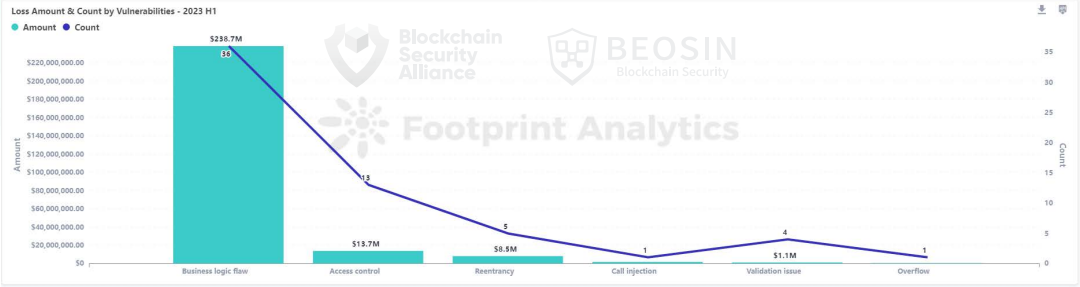
In the first half of 2023, the most frequent attack type with the highest loss amount was contract vulnerability exploits. A total of 60 contract vulnerability exploits resulted in losses of $264 million, accounting for 56% of the total losses.

Approximately $100 million worth of security incidents were categorized as "Unclear" in terms of attack types. This includes events such as the theft of $67 million from the Atomic Wallet and a $20 million attack on the cryptocurrency brokerage firm FPG. These incidents involve significant amounts of funds and affect numerous users. It is recommended that projects actively collaborate with third-party security companies, promptly disclose investigation results, take necessary remedial measures, and assume responsibility for the security of user assets while investigating the causes of such events.

Additionally, there were 7 incidents of private key compromise, resulting in losses of approximately $27.67 million. In 2022, private key compromise also ranked third among all attack types. Private key compromise continue to pose a threat to project security. Strengthening the professional ethics and security awareness management of core team members is particularly important, as evidenced by some incident disclosures.



Loss Amount by Attack Type (%)



Loss Amount by Attack Type (%)

In terms of vulnerability types, the top three causes of losses were business logic flaws, access control, and reentrancy. **A total of 36 business logic vulnerabilities resulted in losses of approximately $239 million, accounting for 90% of all losses caused by contract vulnerabilities.** These types of vulnerabilities are often overlooked by developers and can lead to significant losses once exploited. In fact, 9 incidents had losses exceeding $1 million each. It is recommended that project teams seek experienced professional auditing firms to conduct audits.

6. Typical Security Incidents in H1 2023

6.1 Euler Finance

Overview

On March 13th, the Ethereum-based lending project Euler Finance fell victim to a flash loan attack, resulting in a loss of $197 million.

On March 16th, Euler offered a $1 million reward for information that could help in the arrest of the hackers and the return of the stolen funds.

On March 17th, Euler Labs CEO Michael Bentley tweeted that "Euler has always been a security-conscious project". Between May 2021 and September 2022, Euler Finance underwent ten audits conducted by six blockchain security firms, including Halborn, Solidified, ZK Labs, Certora, Sherlock, and Omnisica.

Starting from March 18th until April 4th, the attacker began returning the stolen funds in installments. During this time, the attacker apologized through on-chain messages, admitting to having "messed with others' money, others' work, others' lives" and asking for forgiveness.

Txn Type: **2 (EIP-1559)** Nonce: **60** Position In Block: **12**

```
Jacob here. I don't think what I say will help me in any way but I still want to say it. I fucked up. I
didn't want to, but I messed with others' money, others' jobs, others' lives. I really fucked up. I'm sorry.
I didn't mean all that. I really didn't fucking mean all that. Forgive me.
```

On-chain Message from Euler Hacker

On April 4th, Euler Labs announced on Twitter that, after successful negotiations, the attacker had returned all the stolen funds.

Vulerability Analysis

In this attack, the donateToReserves function of the Etoken contract failed to properly verify the actual amount of tokens held by the user and the health status of the user's ledger after the donation. The attacker exploited this vulnerability by donating 100 million eDAI while actually having only deposited 30 million DAI.

As a result of the donation, the health status of the user's ledger met the liquidation criteria, triggering the liquidation of the lending contract. During the liquidation process, eDAI and dDAI were transferred to the liquidation contract. However, due to the large amount of bad debt, the liquidation contract applied the maximum discount for liquidation. After the liquidation was complete, the liquidation contract held 310.93 million eDAI and 259.31 million dDAI.

At this point, the health status of the user's ledger was restored, and the user could withdraw funds. The amount that could be withdrawn was the difference between eDAI and dDAI. However, there were only 38.9 million DAI actually available in the pool, so users could only withdraw this portion of the funds.

```
354   function donateToReserves(uint subAccountId, uint amount) external nonReentrant {
355       (address underlying, AssetStorage storage assetStorage, address proxyAddr, address msgSender) = CALLER();
356       address account = getSubAccount(msgSender, subAccountId);
357
358       updateAverageLiquidity(account);
359       emit RequestDonate(account, amount);
360
361       AssetCache memory assetCache = loadAssetCache(underlying, assetStorage);
362
363       uint origBalance = assetStorage.users[account].balance;
364       uint newBalance;
365
366       if (amount == type(uint).max) {
367           amount = origBalance;
368           newBalance = 0;
369       } else {
370           require(origBalance >= amount, "e/insufficient-balance");
371           unchecked { newBalance = origBalance - amount; }
372       }
373
374       assetStorage.users[account].balance = encodeAmount(newBalance);
375       assetStorage.reserveBalance = assetCache.reserveBalance = encodeSmallAmount(assetCache.reserveBalance + amount);
376
377       emit Withdraw(assetCache.underlying, account, amount);
378       emitViaProxy_Transfer(proxyAddr, account, address(0), amount);
379
380       logAssetStatus(assetCache);
381   }
382 }
```

Vulnerability of Euler Incident

6.2 BonqDAO

Overview

On February 1st, DeFi protocol BonqDAO fell victim to a price manipulation attack. The attacker minted 100 million BEURs and then swapped for other tokens on Uniswap. The ALBT price dropped to almost zero, which further triggered the liquidation of ALBT vaults. Based on the token prices at the time of the attack, the loss was as high as $88 million. However, due to drained liquidity, the actual loss was around $1.85 million.

Vulerability Analysis

In this attack, the attacker carried out two types of attacks: one involving borrowing a large number of tokens by manipulating prices, and the other involving profiting by manipulating prices to liquidate others' assets.

The BonqDAO platform's oracle used the 'getCurrentValue' function instead of 'getDataBefore'. The hacker became a price reporter by staking 10 TRB tokens (worth only about $175) and manipulated the price of the WALBT token in the oracle by calling the submitValue function. After setting the price, the attacker called the createTrove function in the Bonq contract, created a trove contract, and deposited 0.1 WALBT for borrowing. Normally, the borrowing limit should be less than the price of 0.1 WALBT, ensuring that the stake ratio remains within a safe range. However, in this borrowing process, the collateral value was calculated using the TellorFlex contract. In the previous step, the attacker had already set an exceptionally high price for WALBT, resulting in the attacker borrowing 100 million BEUR tokens in this transaction.

In the second transaction, the attacker set the WALBT price exceptionally low, allowing them to liquidate the WALBT tokens staked by other users at a minimal cost.

6.3 Platypus Finance

Overview

On February 17th, Platypus Finance on Avalanche was exploited due to a checking mechanism flaw, resulting in a loss of approximately $8.5 million. However, the attacker did not implement a withdrawal function in the contract, leaving the attack proceeds stuck within the attack contract and unable to be withdrawn.

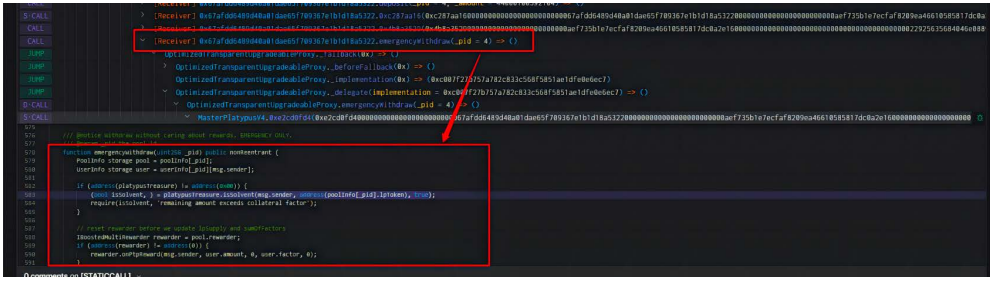
On February 23rd, Platypus announced that they had contacted Binance and confirmed the hacker's identity. Platypus also stated that they would repay at least 63% of the funds to users.

On February 26th, the French National Police arrested and summoned two suspects believed to have attacked Platypus.

Vulerability Analysis

The cause of the attack was a flaw in the checking mechanism of the emergencyWithdraw function in the MasterPlatypusV4 contract. It only checked whether the user's borrowing amount exceeded their borrowLimitUSP (borrowing limit) but did not verify whether the user had repaid their debt.

The attacker first used the AAVE contract to flashloan 44 million USDC and deposited it into the Pool contract, then minted 44 million LP-USDC. Next, the attacker called the borrow function to borrow 41.79 million USP and immediately called the EmergencyWithdraw function afterward.



Vulnerability of Platypus Incident

Within the EmergencyWithdraw function, there is an isSolvent function to check if the balance exceeds the maximum amount that can be borrowed. If it returns true, it proceeds with the transfer operation without considering whether the debt has been repaid. Thus, the attacker was able to successfully call the function and withdraw the previously deposited 44 million LP-USDC without repaying the debt.

6.4 Yearn Finance

Overview

On April 13, 2023, Yearn Finance's yusdt contract fell victim to a flash loan attack, resulting in the hacker profiting over $10 million. It appears that the yUSDT contract was mistakenly configured during its deployment over 1,000 days ago. It was erroneously deployed using Fulcrum iUSDC instead of Fulcrum iUSDT.

On May 26, the Yearn attacker transferred 4,134 ETH to Tornado Cash.

Vulerability Analysis

The attack primarily exploited a misconfiguration in the yUSDT token contract. During the rebalance process for selecting pools, only USDT tokens were used as the add amount, while USDC tokens were not considered valid for pool addition. As a result, when the attacker used USDC to "consume" all the USDT in the contract, the pool balance became zero, allowing the attacker to mint a significant amount of tokens.

```
679  function rebalance() public {
680    Lender newProvider = recommend();
681
682    if (newProvider != provider) {
683      _withdrawAll();
684    }
685
686    if (balance() > 0) {
687      if (newProvider == Lender.DYDX) {
688        supplyDydx(balance());
689      } else if (newProvider == Lender.FULCRUM) {
690        supplyFulcrum(balance());
691      } else if (newProvider == Lender.COMPOUND) {
692        supplyCompound(balance());
693      } else if (newProvider == Lender.AAVE) {
694        supplyAave(balance());
695      }
696    }
697
698    provider = newProvider;
699  }
```

```
556  function balance() public view returns (uint256) {
557    return IERC20(token).balanceOf(address(this));
558  }
```

Vulnerability of Yearn Finance Incident

6.5 MEV bot

Overview

On April 3, 2023, multiple MEV bots fell victim to a malicious sandwich attack, resulting in a loss of approximately $25 million.

Sandwich attacks are a popular front-running technique in DeFi. To execute a "sandwich" trade, an attacker (referred to as a predatory trader) identifies a pending victim transaction and attempts to sandwich that victim by placing their own transactions before and after it. This strategy exploits the buy and sell orders to manipulate asset prices.

The objective of a sandwich trade is to take advantage of the unexpected slippage experienced by the victim. Additionally, there are many bait bots that utilize MEVBot's strategies in reverse, employing tactics such as malicious bait tokens or specific amounts in transfer functions. In this particular attack, vulnerabilities related to the MEVBot were exploited.

Vulerability Analysis

The malicious node leveraged vulnerabilities associated with MEV-boost-relay to manipulate prices through a malicious sandwich attack and ultimately profit. Normally, it would be difficult for a malicious proposer to modify bundles due to double-signing penalties. However, the attack involved setting the parent_root and state_root to 0x00, causing Publish-Block to return an error. Due to a lack of error handling in older versions, this allowed access to the disclosed bundles, leading to the occurrence of the event.

```
983  978
     979  +        // Publish the signed beacon block via beacon-node
     980  +        signedBeaconBlock := SignedBlindedBeaconBlockToBeaconBlock(payload, getPayloadResp)
     981  +        code, err := api.beaconClient.PublishBlock(signedBeaconBlock) // errors are logged inside
     982  +        if err != nil {
     983  +                log.WithError(err).WithField("code", code).Error("failed to publish block")
     984  +                api.RespondError(w, http.StatusBadRequest, "failed to publish block")
     985  +                return
     986  +        }
     987  +
     988  +        // give the beacon network some time to propagate the block
     989  +        time.Sleep(time.Duration(getPayloadResponseDelayMs) * time.Millisecond)
     990  +
984  991          api.RespondOK(w, getPayloadResp)
985  992          log = log.WithFields(logrus.Fields{
986  993                  "numTx":       getPayloadResp.NumTx(),
     ↓ ↑      @@ -1014,16 +1021,6 @@ func (api *RelayAPI) handleGetPayload(w http.ResponseWriter, req *http.Request)
1014 1021                          log.WithError(err).Error("failed to increment builder-stats after getPayload")
1015 1022                  }
1016 1023          }()
1017      -
1018      -        // Publish the signed beacon block via beacon-node
1019      -        go func() {
1020      -                if api.ffDisableBlockPublishing {
1021      -                        log.Info("publishing the block is disabled")
1022      -                        return
1023      -                }
1024      -                signedBeaconBlock := SignedBlindedBeaconBlockToBeaconBlock(payload, getPayloadResp)
1025      -                _, _ = api.beaconClient.PublishBlock(signedBeaconBlock) // errors are logged inside
1026      -        }()
1027 1024  }
1028 1025
```

Vulnerability of MEV bot Incident

The attacker first targeted pools with low liquidity to test whether the MEV bot would front-run the transactions. Once the attacker successfully executed the test, they utilized a large quantity of tokens previously swapped in Uniswap V3 to perform swaps within low-liquidity V2 pools. They enticed the MEV bot to use all of its WETH in a front-running purchase of low-value tokens. However, the transaction that was front-run was actually an attack transaction aimed at the MEV, swapping a significant amount of tokens for the WETH that the MEV had just used for the front-run. As a result, when the MEV bot attempted to swap the WETH back, it failed because the attack transaction had already swapped the WETH.

7. Typical AML Security Incident

Atomic Wallet $67 Million theft incident

On June 3, several Atomic Wallet users reported on social media that their wallet funds had been stolen. The attack caused a loss of at least about $67 million. The theft involved a total of 21 chains, including BTC, ETH and TRX. The stolen funds were mainly concentrated in the ethereum chain.

Ethereum

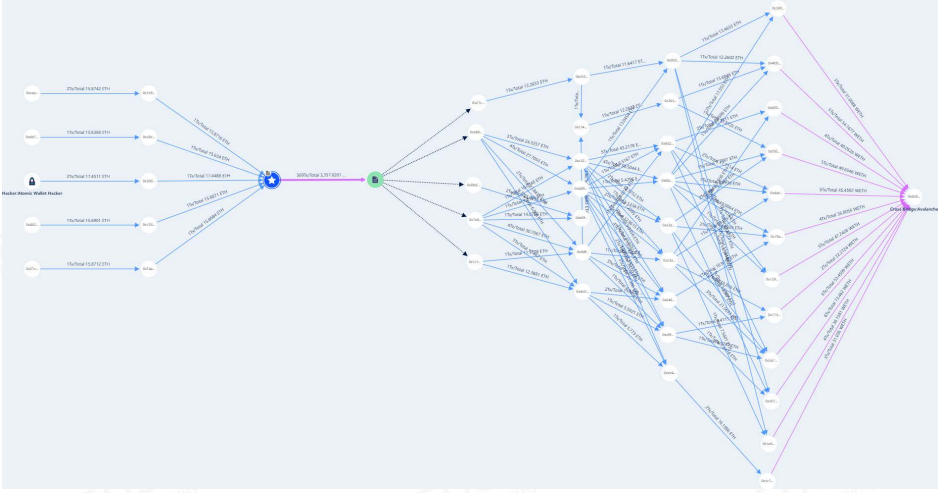
There are two main money laundering methods on Ethereum:

1.Money Laundering through Contract Diversification and Avalanche Cross-Chain

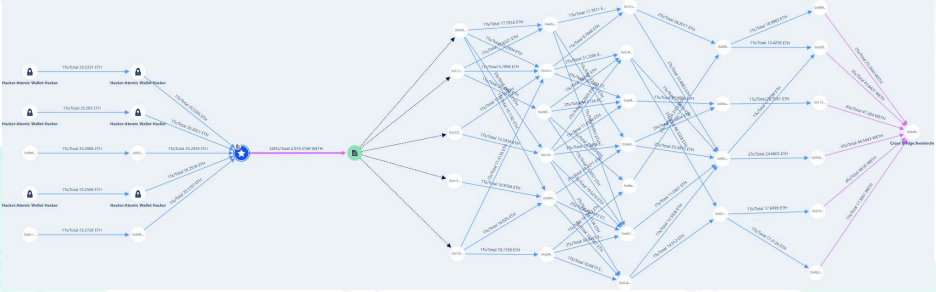
Hackers first convert valuable coins into the native currency of the public blockchain. Then, they utilize two contracts for aggregation.

The contract address consolidates ETH by converting it into WETH through two layers of transfers. The WETH is then transferred to a contract used for contract diversification, which facilitates cross-chain operations by transferring up to five layers deep into the wallet address on Avalanche. This cross-chain operation does not involve contracts but rather internal accounting transactions within Avalanche.

Consolidation Contract 1:



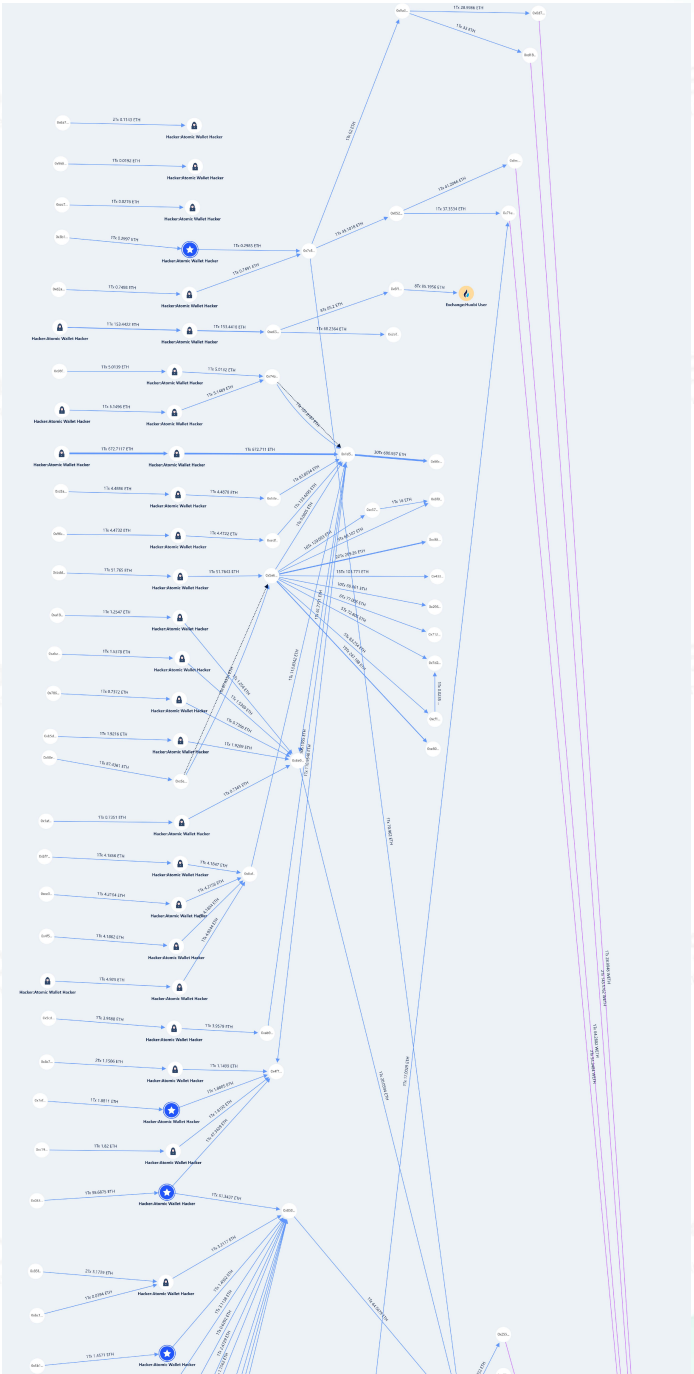
Consolidation Contract 2:

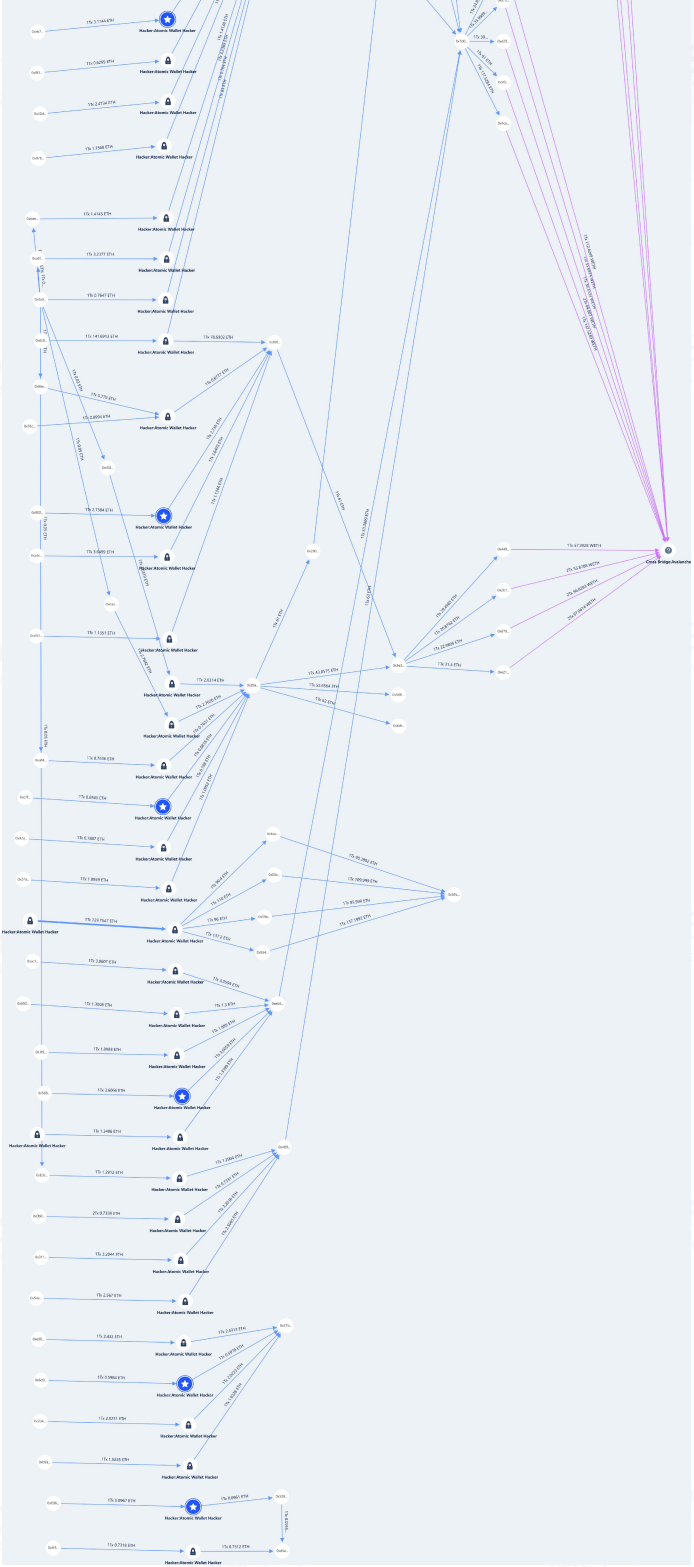


2.Direct Diversification without Contracts and Launder through Various Cross-Chain Bridge Protocols and Exchanges

This portion of money laundering involves directly diversifying funds without the use of contracts and utilizing various cross-chain bridge protocols and exchanges.

The total amount involved in this part is currently recorded as 9,896 ETH, which will be consolidated through multiple aggregation addresses. The financial linkage diagram is as follows:

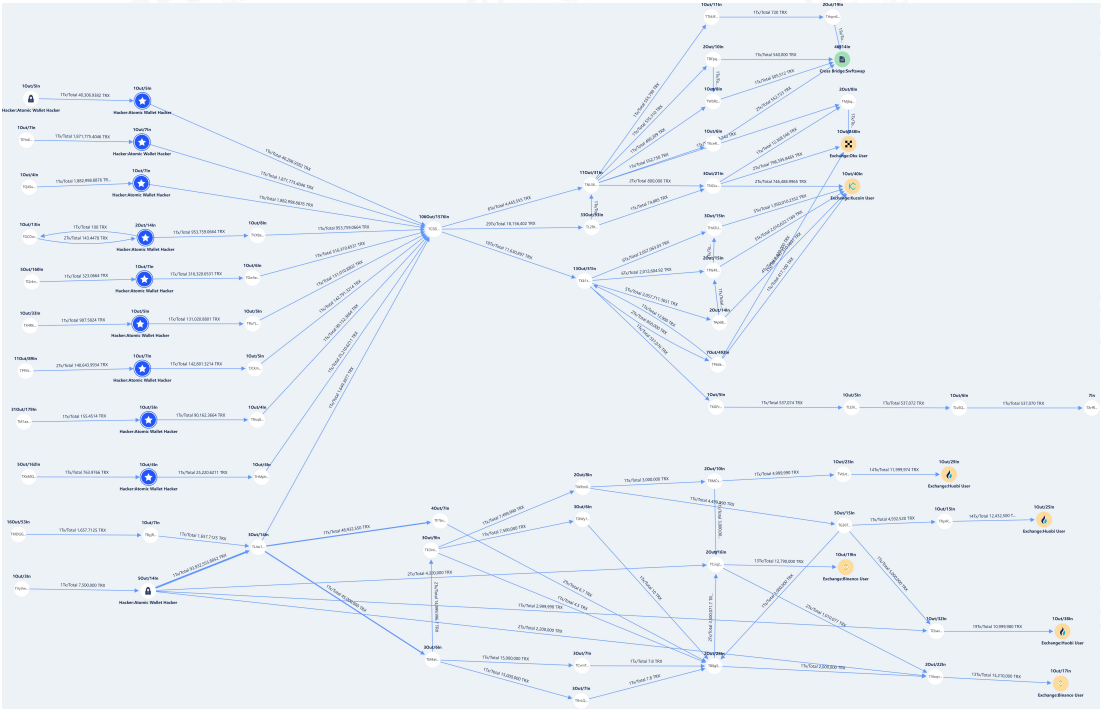




TRON

Similar to the Ethereum chain, on TRON, stolen wallet virtual currencies are converted entirely into TRX through two layers of addresses before being further transferred. However, in contrast, the aggregation addresses are not contract-based but rather regular addresses. After diversification, the funds are transferred to various exchange deposit addresses. Some of the stolen funds remain on the chain without being transferred, and there are numerous consolidation addresses.

It can be observed that there are multiple money laundering channels used by hackers, primarily involving laundering through various exchange accounts. There are also cases where funds are directly flowing into cross-chain bridge contracts.



Beosin KYT – TRON

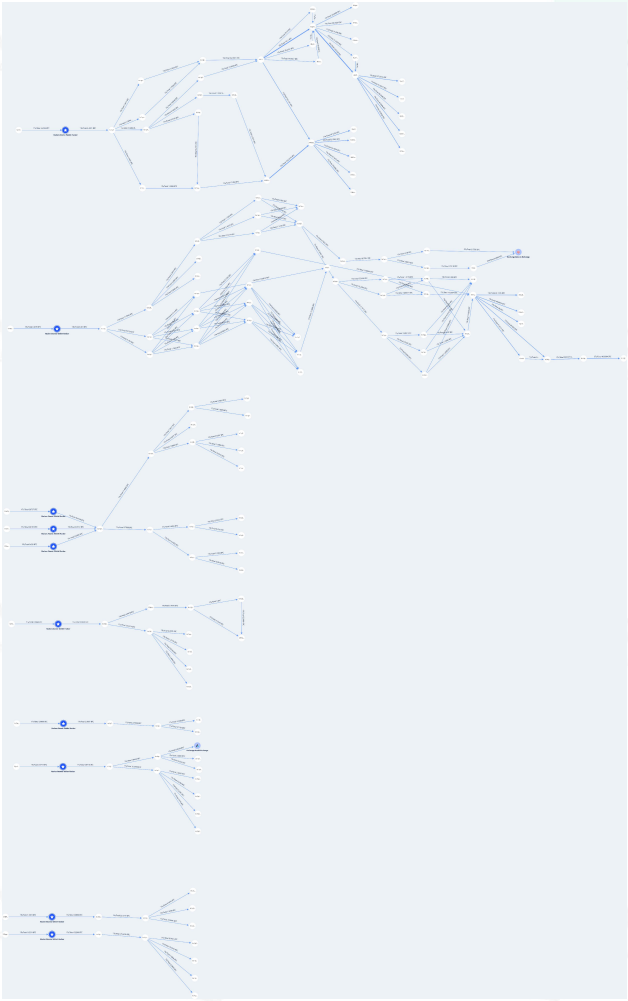
BTC Chain

The known aggregated addresses involved in BTC contain a total of 420.882 BTC.

In the BTC chain, the addresses are distributed across multiple aggregation addresses. After consolidation, there is no cross-flow of funds between these addresses, indicating the existence of numerous consolidation addresses.

Similar to other chains, stolen wallet funds are directly transferred to hacker-controlled addresses. The hacker then controls the funds and transfers them through one layer of intermediaries to aggregation addresses for subsequent diversification. The diversification process involves at least four layers, after which the funds may be deposited or mixed into suspected money laundering addresses with larger transaction volumes.

The route pattern is shown in the diagram below:



Beosin KYT – BTC

In recent years, crimes involving virtual assets such as cybercrime, money laundering, and dark web transactions have become increasingly common. The decentralized, open, and anonymous nature of blockchain poses significant challenges for regulatory authorities.

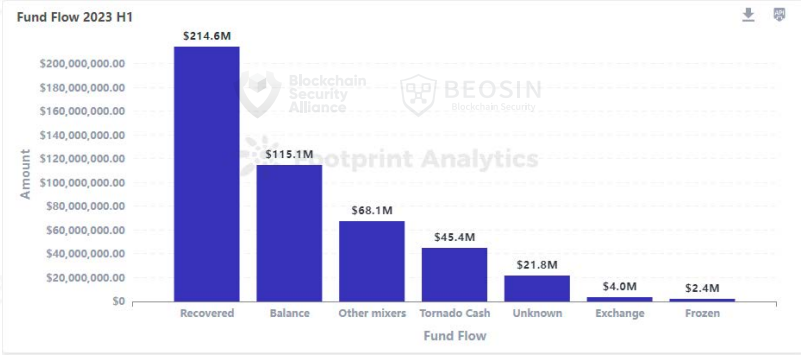
To address these issues, various security institutions, represented by Beosin, have proposed a solution known as KYT (Know Your Transactions). The purpose of KYT is to enable trading platforms and regulatory agencies to understand every transaction on the blockchain. In traditional financial transactions, financial service providers design anti-money laundering systems through Know Your Customer (KYC) procedures and transaction data analysis. In the virtual asset trading realm, trading platforms can utilize KYC and KYT technologies to associate each transaction with the entities involved, analyze their transaction behavior, identify criminal patterns, and use on-chain analysis and tracking tools to trace and profile each transaction, as well as rate users, thus reducing the risk of criminals laundering virtual assets.

Beosin KYT provides customized compliance solutions based on the specific needs and capabilities of users. In addition to features such as black address queries, sanctions list filtering, address/transaction risk scoring, address monitoring and alerting, and tracking and investigation capabilities, Beosin KYT also offers customized risk strategy management, AI-powered visualization of virtual asset path, and STR (Suspicious Transaction Report) export functionalities. It has already provided services to institutions, exchanges, wallet companies, and other entities in multiple countries and regions. Its collaborative clients include Binance, OKX, HashKey Group, and others.

8. Stolen Fund Flow

45.5% of stolen assets were recovered

In the first half of 2023, according to Beosin KYT, a virtual asset anti-money laundering compliance and analysis platform, **approximately $215 million of stolen assets were recovered, accounting for 45.5% of all stolen assets.** In contrast, in 2022, only 8% of stolen assets were recovered. The chances of fund recovery have significantly increased in 2023. In addition to negotiations with hackers for recovery, there has been an increase in cases where recovery is achieved through the combined efforts of security firms, law enforcement agencies, and community involvement. Furthermore, the improvement of global regulatory systems and increased enforcement efforts have acted as a deterrent to hacker activities.



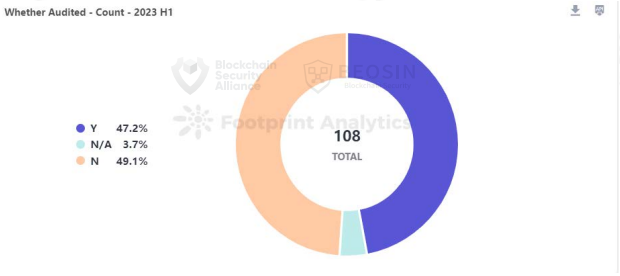
Stolen Fund Flow 2023 H1

Approximately $113 million of stolen assets were transferred to mixers. Among them, approximately $45.38 million was transferred to Tornado Cash, and approximately $68.14 million to other mixer platforms. Since Tornado Cash faced sanctions by the U.S. Office of Foreign Assets Control (OFAC) in August 2022, the total amount of funds mixed using Tornado Cash has significantly decreased. However, the usage of other mixer platforms such as FixedFloat and Sinbad has noticeably increased.

9. Audit Status Analysis

The proportion of audited and unaudited projects is roughly equal

Out of the 108 attacked projects, 51 had undergone audits, while 53 had not. The proportion is roughly the same as in 2022.



Whether Audited by Count

Among the 51 audited projects, 31 (60%) were attacked due to contract vulnerabilities. This ratio is higher than last year's 45%, indicating that the quality of the entire audit market is still not optimistic. It is recommended that project teams must seek professional security companies for auditing.

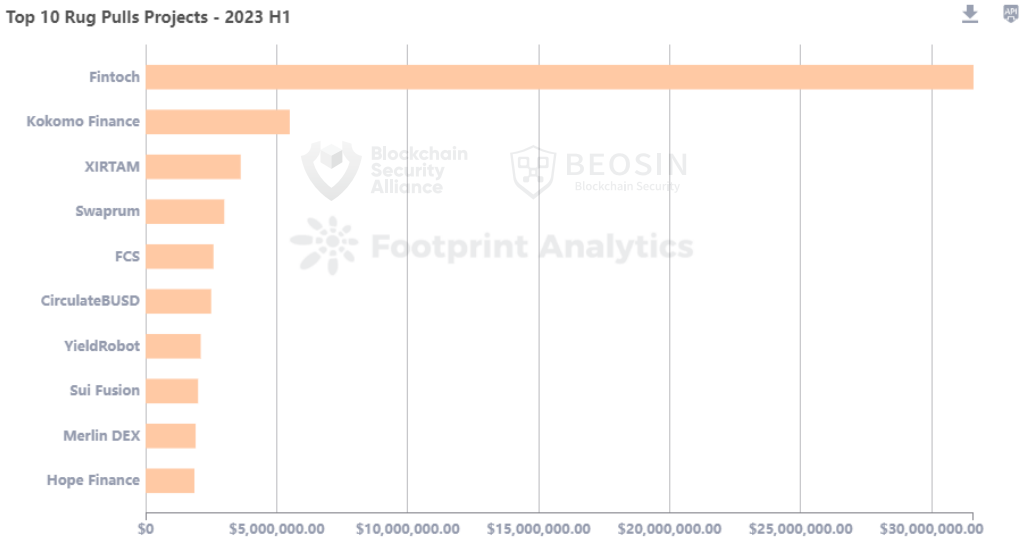
10. Rug Pulls

$75.87 million lost in 110 rug pulls

In the first half of 2023, the Web3 domain witnessed a total of 110 major Rug Pull events, involving approximately $75.87 million.

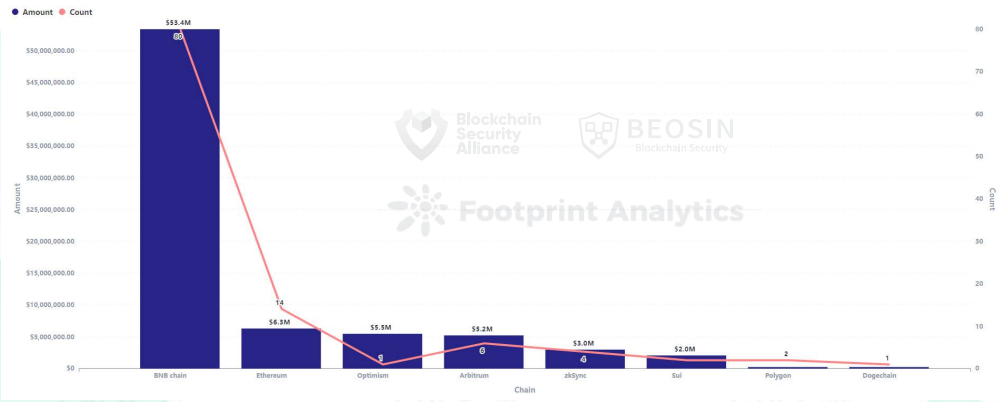
In terms of the amount involved, there were 14 Rug Pull events (12.7%) with amounts exceeding $1 million, 41 events (37.3%) in the range of $100,000 to $1 million, and 55 events (50%) with amounts below $100,000.

The largest Rug Pull event in terms of the amount was the Fintoch project, which took away approximately $31.6 million in assets.



Top 10 Rug Pulls H1 2023

In terms of blockchains, BNB Chain experienced 80 Rug Pull events, involving an amount of $53.37 million, which was significantly higher than other public blockchains.



Rug Pulls by chain

11. Summary

Overall, total losses from hacks in the Web3 space have declined significantly compared to 2022. In the first half of 2022, the total loss from attacks was approximately $1.91 billion, which decreased to around $1.69 billion in the second half of 2022. However, in the first half of 2023, this value dropped to $470 million, and approximately $215 million of stolen assets were recovered. Hacks have exhibited a substantial slowdown, and the main reasons contributing to this phenomenon include the gradual improvement of global regulatory systems, increased law enforcement efforts, improved security awareness among projects, the sanctioning of Tornado Cash, and enhancements in anti-money laundering (AML) technology and procedures. Additionally, there have been cases where the community has relied on off-chain intelligence to identify hacker identities and force them to return stolen funds.

Despite the significant slowdown in hacker attacks, smart contract security issues cannot be ignored. In the first half of 2023, the most frequent and financially impactful attack type was the exploitation of smart contract vulnerabilities. A total of 60 smart contract vulnerability incidents resulted in losses of $264 million, with the majority of vulnerabilities being related to business logic flaws. Some complex business logic vulnerabilities require experienced professional auditing firms to identify. Beosin auditing team conducts in-depth analysis of every hacking incident (on Twitter @BeosinAlert), ensuring that the knowledge and technology derived from these incidents are applied to the auditing process to address any potential attacks.

Contrary to the declining trend of hacker attacks, phishing scams targeting ordinary users have become more frequent. In the first half of 2023, a series of wallet drainer groups, led by Venom Drainer, emerged. They developed malicious toolkits for sale, and buyers would share profits with them after successfully phishing victims. Such phishing scams have affected a wide range of users, with Venom Drainer alone victimizing at least 15,000 individuals. For ordinary users, it is advisable to regularly pay attention to security company alerts, systematically learn about anti-phishing and anti-theft practices, and consider installing anti-phishing plugins, transaction pre-execution tools, and other reminders (while not solely relying on tools, as strengthening one's own security awareness always takes precedence).

II.
H1 2023 Top 10 Hotspots in Web3

This chapter was written by Jesse Zheng@SUSS NiFT and Fishery Isla @Biteye

1. Ethereum Shanghai Upgrade

The most important event of Ethereum in the first half of this year is the Shanghai upgrade. This is the last important step in the transition of Ethereum from Proof of Work (PoW) to Proof of Stake (PoS).

After seven months of the "merge" upgrade of Ethereum, Ethereum performed "Shanghai-Capella" upgrade on April 12 (enabling stakers who did not provide withdrawal certificates at the time of initial deposits to have the ability to provide certificates, so as to realize withdrawals), bringing the withdrawal function to the execution layer, enabling stakers to withdraw the 18 million ETH they have locked since 2020 from the beacon chain to the execution layer, and realize the optional full withdrawal or staking income withdrawal to release the liquidity of staked ETH. This enhanced investors' confidence in Ethereum and also improves the security of the Ethereum network.

In addition, although the Shanghai upgrade cannot reduce the gas fee, the implemented EIP-3651, EIP-3855, and EIP-3869 reduce the gas fee for Ethereum developers and block creators.

After the Shanghai upgrade, although some early stakers have withdrawn funds, overall, the net inflow of staking is still greater than the net outflow and the number of staked ETH and validators shows an accelerated upward trend.

Ethereum continues to improve its blockchain performance through steady technological upgrades and brings confidence to users and investors. The market has also begun to build financial infrastructure around staked ETH. Projects such as LSD-based stablecoin issuance, flash loan leverage, and income enhancement have received widespread attention.

However, currently Lido occupies 31% of the staking market share, the Ethereum ecosystem needs to promote decentralized node technology and attract more outstanding staking service providers to participate to reduce the risk of network centralization.

2. Which Layer2 is more popular?

On June 12, Vitalik Buterin pointed out in his latest blog that the scaling of Layer2 is one of the important technologies for Ethereum to develop sustainably in the long run. If Ethereum is a kingdom, then Layer2 is the states under this kingdom. The development of the states is related to the rise and fall of the kingdom.

According to L2beat, Arbitrum and Optimism have gained an advantage with Optimism Rollup, a more mature Rollup technology, with a market share of about 64.55% and 18.58% respectively and a dominant position in the Layer2 market. Users received Arbitrum airdrop on March 23 and the huge wealth effect further enhanced users' belief in the Ethereum community.

Other noteworthy events:

1. Optimism completed the Bedrock mainnet upgrade on June 7, which further reduced transaction fees, shortened the system delays, and improved node performance.

2. Coinbase launched Layer2 Base based on OP Stack, but does not plan to issue a native token and plans to release the mainnet this year.

3. Another scaling technology of L2, Zero Knowledge Rollup, has also made important progress.

4. Type1 zkEVM: Taiko launched the Alpha-3 incentive test network on June 7, mainly testing the economic incentives of the protocol, the interaction between the proposer, the prover, and the protocol, and the Taiko initial layer (L3).

5. Type-2 zkEVM: The main projects of this track are Scroll, Linea and Polygon zkEVM.

1) The Beta version of the Polygon zkEVM mainnet was launched as scheduled on March 27, using ETH to pay for gas and MATIC for staking and governance.

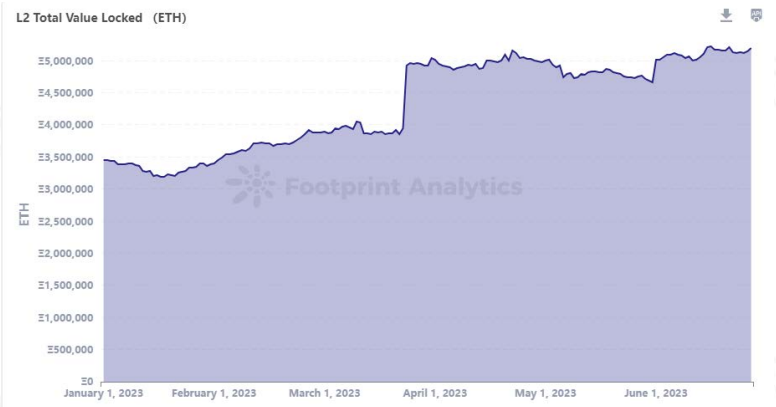
2) Scroll and the Ethereum Foundation jointly developed an open source zkEVM and it is expected to launch the mainnet in Q3.

3) Linea is expected to launch the mainnet in July, with the development focus on Multi Prover and Layer3.

6. Type-3 zkEVM: Kakarot has achieved 100% bytecode equivalence and is about to transition to Type 2.5. Kakarot is working on deploying zkEVM as Layer3 on Starknet.

7. Type-4 zkEVM: The zkSync Era mainnet was open to everyone on March 24. At present, the interaction costs are relatively high and most of projects are natively built on zkSync Era. Most blue-chip protocols have not yet been deployed. Another Type-4 star project, Starknet, underwent a mainnet upgrade in June to officially activate Cairo 1, update the sequencer, and improve scaling and transaction delays, but the overall user experience still needs to be improved.

The TVL denominated in ETH on Layer2 increased from approximately 3.45 million at the beginning of the year to 5.20 million in June. The trend of transactions shifting to Layer2 continues.



L2 TVL – 2023 H1

However currently all Layer2 transactions per second are lower than that of Ethereum. Except for the first few Layer2 blockchains, the number of transactions on most Layer2 are very low. In the second half of the year, there are multiple Layer2 blockchains that plan to launch the mainnet. Whether so many Layer2s are needed in the market remains to be a question.

L2 TPS

Name	Past Day Tps	7D Change	Max Daily Tps	30D Count	Data Source
dYdX	4.7	78.7%	11.45on 2022 Feb 15	8.1M	Closed API
Immutable X	1.74	-10.55%	39.35on 2022 Mar 11	5.66M	Closed API
ApeX	0.93	-10.54%	1.38on 2023 Apr 13	2.69M	Closed API
Sorare	0.42	7.55%	2.31on 2022 Oct 23	918K	Closed API
Myria	0.12	-16.26%	10.27on 2023 Jun 16	3.8M	Closed API
rhino.fi	0.03	-14.13%	0.42on 2021 Dec 02	78.77K	Closed API
Starknet	1.97	53.48%	3.05on 2023 May 16	4.73M	Explorer API
zkSync Lite	1.23	44.85%	3.29on 2023 Mar 21	2.46M	Explorer API
Loopring	0.05	-16.35%	1.48on 2022 Jul 12	118K	Explorer API
Aztec	0	0%	0.05on 2021 Dec 17	76	Explorer API
Ethereum	11.54	-4.72%	22.37on 2022 Dec 09	31.61M	Blockchain RPC
zkSync Era	10.12	22.82%	12.00on 2023 May 16	21.31M	Blockchain RPC
Arbitrum One	10.11	16.22%	31.64on 2023 Mar 23	25.02M	Blockchain RPC
OP Mainnet	6.9	39.8%	9.26on 2023 Jan 12	12.96M	Blockchain RPC

Rows 1-14 of 19

L2 TPS

3. Ecosystem of Move-based blockchain will rise or fall?

At the beginning of 2023, with the gradual improvement of the macro environment, Ethereum also announced the definite time for the Shanghai upgrade, and the entire secondary market had a bull market for nearly a quarter.

2023 H1 Crypto MarketCap

The market at the beginning of the year mainly revolved around the hype in the secondary market. Meme coins and the primary market are relatively dull. The Move-based blockchain Aptos performed the most prominently in this wave, with a circulation market value of 500 million dollars, which rose to 3 billion dollars in just 20 days, leading a wave of "unlocking pump". After a pump in a short period of time, Aptos continued to decline, similar to most altcoins and has returned to the price when FTX collapsed. On the other hand, Sui, another star project of Move-based blockchains, reached its peak when it was launched and its price continued to fall.

The Move-based blockchain represents a different scaling development direction from Ethereum Layer2. The security and flexibility of Move have become one of the main advantages of the new blockchains. At present, the Move-based blockchains are still in a very early stage. The projects using the Move language include: Aptos, Sui, 0L Network, and Starcoin. These four projects have all launched their mainnet so the Move developers can have real benefits, which helps to attract more developers and reserve power for the next bull market. Also, it's worth saying that Move, as a new programming language, will take time to prove its stability. Beosin recently discovered the severity level vulnerability of Move VM, which can lead to the collapse of the entire network of blockchains such as Sui and Aptos. At present, this vulnerability has been fixed.

In the short term, the token distribution of Move-based blockchains is too concentrated. The number of unlocked tokens is large and the token price fluctuates violently, which has certain risks. In the long run, due to the various advantages of Move over Solidity, its market share should have a chance to be greatly improved in the next bull market. As a new force, it will compete with the traditional blockchains that have passed the test of time.

4. Blur drives an NFT bull market

In the NFT market in February, the most eye-catching thing was the launch of $BLUR. Blur's bidding mining mechanism not only allowed a large number of users to obtain $BLUR airdrops, but also provided great liquidity into the NFT market, which brought an NFT bull market and had a profound impact on the products of the NFT track.

The biggest impact is that due to the dense bidding orders, NFT whales have the opportunity to exit. These whales used to hold a huge amount of blue-chip NFT series at a very low cost, but failed to exit due to the lack of liquidity during the Opensea monopoly market period. A large number of NFT selling not only has high friction costs, but is also very likely to dump the entire NFT market. Therefore, BLUR provides a good opportunity for NFT whales to exit. Whales may be large institutions, KOLs, etc. After their exit, the popularity of BLUR declines.

After this wave, with the changes in the psychology of new NFT holders, a decreasing BLUR's bidding mining revenue, and other factors, the liquidity of the NFT market has begun to shrink again.

In the past six months, there were some opportunities in the NFT market, such as Milady Maker and Pudgy Penguins. The commonality of these two projects is that the community is very active and the team continue to develop markets. Community culture is the core of NFT. It can be seen that the market still buys the NFT community narrative. It can be seen that the clear development direction of NFT will promote the long-term development of Web3.

5. How AI products such as ChatGPT affect Web3

In the past six months, AI has once again become a hot spot in the VC firms in tech. For a long time, the investment funds of Web3 and AI have partly overlapped, which means that if AI continues to be popular, the funds of Web3 track will be relatively reduced. Therefore, the teams building Web3 projects are trying their best to move their narratives closer to AI, or use AI to improve team productivity.

Therefore, how to use AI will be a topic that teams in Web3 are unable to avoid in the future. Here are some trends that are happening:

1. Smart contract audit by AI

Before the launch of ChatGPT, some smart contract audit team used AI to complete the initial review of contracts to find some basic bugs and team members would complete the final audit report.

Now ChatGPT is more powerful than any previous AI. Thus, many people hope that AI can complete a highly reliable smart contract audit. An organization recently conducted an experiment to compare ChatGPT with 28 Ethernaut challenges, to see if it can identify smart contract vulnerabilities. Of the 23 challenges introduced before the Chatgpt training data cut-off date of September 2021, GPT successfully solved 19. While this is an impressive result, GPT performed poorly on the latest level of Ethernaut, failing 4 out of 5 questions. This shows that while AI can be used as a tool to find certain security vulnerabilities, it is currently not able to replace the need for human auditors.

For a security company like Beosin, based on the company's rich smart contract security dataset, it is possible to train and fine-tune an intelligent model that can deeply understand the logic of the smart contract with the help of the ChatGPT basic large model, which further improves the ability of VaaS, a formal verification tool, to detect and verify the security issues of complex business contracts.

2. AI replaces positions in the Web3 team

Just as the emergence of ChatGPT has caused many people to experience unemployment anxiety and worry that their jobs will be completely replaced by AI, Web3 builders also have the same worries. Although it is cruel, from the perspective of investors in the Web3 industry, the trend of using AI to replace Web3 team members may come faster than imagined. On April 23, Rhett Mankind, a digital artist, tweeted that he provided ChatGPT with instructions and a budget of $69, allowing ChatGPT to independently issue a memecoin. At the same time, the author introduced a series of processes such as an AI tool to decide the memecoin name in detail on YouTube. In addition, the AI tool also wrote the smart contract code of the project. The market bought into this theme very much. After a few days of hype, the market value of the project exceeded 50 million dollars. Although the experience of this meme project may not be replicated, it can inspire us to use AI to achieve the optimization of jobs in Web3.

6. The collapse of crypto-friendly banks

In March, the U.S. banking industry suffered a severe crisis. Crypto-friendly banks Silvergate Bank, Silicon Valley Bank and Signature Bank have collapsed one after another. The failures of Silicon Valley Bank and Signature Bank regarded as the second and third largest bank collapses respectively in U.S. history.

Silvergate suffered a run after the FTX collapse because it accepted too many deposits from the crypto industry. Silicon Valley Bank bought a large number of long-term bonds during the low interest rate period, and these bonds were severely discounted during the interest rate hike cycle. Bank runs forced them to sell bonds at a discount, making unrealized losses a reality. Signature Bank has been the target of multiple investigations in the past, and its entry into the crypto market has brought it under increased scrutiny.

On March 11, Circle, the issuer of USDC, admitted that some of its funds were stored in Silicon Valley Bank, which caused panic in the market. USDC fell to 87 cent. Regulators have always been worried that the development of digital assets will have an impact on traditional financial markets, but this time it was a sneak attack on digital assets by traditional financial markets, which set the alarm for risk isolation in the crypto industry.

Interestingly, this banking crisis has once again reminded people of the reason why Satoshi Nakamoto invented Bitcoin: "Banks are trusted to manage money well and allow these wealth to circulate in the form of digital currency but banks use money to create credit bubbles, which shrinks private wealth." Obviously, 15 years later, these bank failures have proved Satoshi Nakamoto's vision to the world and it is indeed difficult for banks to manage money for people. On March 10, the collapse of Silicon Valley Bank pushed inflows into the crypto-related ARK Innovation ETF to $397 million, the fund's largest inflow since April 2021. Some of the original USDC positions in the market were converted into other stablecoins by crypto investors, and some were directly used to buy Bitcoin and Ethereum.

7. Meme season and chaos in altcoins

From the end of April to the first ten days of May, the market is purely a show of memecoins and altcoins.

2023 H1 Crypto MarketCap

It perfectly confirms the old saying that shitcoins are the last FOMO and pump of the market.

In this meme season, there are two successful projects. After their success, there have been many forks.

Pepe

Pepe posted its first tweet on April 5 and listed $PEPE on April 15. Pepe's official twitter stated that they hope to redefine memecoins and change the status of numerous memecoins in the market.

The specific mechanism of Pepe ncludes several aspects. First of all, there is no pre-sale of $Pepe, which means that everyone has an equal opportunity to participate in the project. Second, there is no burn tax on $Pepe, which means that no tokens will be burned during transactions. In addition, Pepe gave up the contract authority, making the issuance and trading of tokens more decentralized. It used pumping to attract the attention of the whole market, and finally listed on Binance on May 6. At the same time, it also reached the highest price in history, and then gradually decreased.

AIDOGE

AIDOGE was launched on April 15 and the project has attracted widespread attention from the market since its launch. The AIDOGE project has grasped the preferences of investors and plans to launch a series of AI NFTs for training, creation and production.

The success of AIDOGE is mainly reflected in several aspects. First of all, it is a decreasing "fair" launch. The reason is that the team can rely on insider information to obtain a huge number of tokens in the early stage. Secondly, AIDOGE can have a high rate of return exceeding the normal level of the market. In addition, when users purchase AIDOGE tokens equivalent to $100-$1000, they can participate in a lucky draw every half hour. This frequency and probability stimulate users to gamble and increase the game in the market.

Compared with Pepe, AIDOGE lacks the price effect of listing on Binance. It peaked on April 30 and then fell all the way.

It can be seen from these two representative altcoins/meme that after the popularity of such projects reached its peak, the possibility of price dumping was high. It was difficult to find a rebound opportunity to stop losses immediately, and the secondary market risk was very high. Don't forget the old saying, a single general achieves fame on the rotting bones of ten thousand. The trend of successful memecoins is the same. There are thousands of forks behind them and the risk of taking over is higher. If you want to invest in such projects, please be prepared to lose all your funds in advance.

8. The recovery of Bitcoin ecosystem

Whenever we talk about hotspots in Web3, BTC always appears. Unlike most projects in the Web3 space, there are a group of developers that are working on Bitcoin for free.

Different from the Ethereum/EVM ecological projects that many people are familiar with, the BTC community is very open. There is no paid small group or the existence of the Ethereum Foundation. Any new developments in the BTC ecosystem will be published in the public forum but the spread of these developments is slow, especially in the Chinese community.

This is the case with Nostr. As early as last year, when former Twitter CEO Jack tweeted support for Bitcoin Layer2/social layer Nostr, Biteye published an article last year to introduce Nostr's groundbreaking. Until February 2023, Nostr and its social app Damus set off a wave. In the past weeks, Damus has been on the cusp again. On June 13, the news that Apple's App Store threatened to remove Damus was spread widely and Damus was suppressed by the world's largest technology giant. It inevitably made the community worry about the future of Nostr. After the communication meeting between Damus and Apple, Damus said that as long as they adjusted the Zaps function, Damus could continue to be listed in the App Store. It is amazing that a decentralized application can communicate with Apple so smoothly. Jack, former Twitter CEO, as an investor in Nostr, has helped Nostr coordinate Web2 and Web3 resources. It is believed to this incident will attract more people's attention to Nostr and raise expectations for the BTC social track.

In the first half of the year, another hotspot in the BTC ecosystem was Ordinals protocol. Based on Ordinals, Brc20 was pioneered to ignite the market and the subsequent micro-innovations like Orc20, GBRC721, and Stamp also received popularity. Although Ordinals does not have a complete set of decentralized solutions and its technology needs to be improved, it still allows users who often follow the BTC community and have the courage to try something new to get high returns.

This market situation enlightens us that the information of the BTC community cannot be ignored and any innovation is worth trying. In the future, we must pay attention to the BTC ecosystem.

9. Hong Kong embraces Web3

Hong Kong used to be the headquarters of many important Web3 organizations, but the undecided policies caused some projects to move their headquarters out of Hong Kong. In the bear market last year, various cryptocurrency exchanges and lending platforms closed down. The United States, Singapore and other countries tightened regulations. Many practitioners and investors were disheartened and believed that the future was bleak. However, at the Hong Kong Financial Technology Week in November 2022, the Hong Kong government issued the "Policy Statement on development of Virtual Assets in Hong Kong", stating that it has an open and inclusive attitude towards virtual asset builders and agrees that Web3 and distributed technologies have the potential to become the trend of financial and commerce trading in the future. This was interpreted by the industry as the beginning of the Hong Kong government's re-embracing of Web3.

In April 2023, Hong Kong hosted the Web3 Festival, which became the largest meeting for crypto enthusiasts in Asia after Covid-19. At the carnival, the Hong Kong government announced a number of policies to support the development of Web3, including Hong Kong's fiscal budget announced the allocation of 50 million hkd to promote the development of the industry, and the fintech internship program for students to encourage more outstanding talents to join the fintech industry.

Compared with Singapore, which does not encourage retail transactions, Hong Kong has adopted a more positive attitude, allowing exchanges to apply for digital asset retail trading licenses for retail investors from June 1, 2023. Banners promoting cryptocurrencies can be seen in public places in Hong Kong. Additionally, Hong Kong has issued tokenized government green bonds and expects to introduce a stablecoin regulatory framework by the end of 2024.

Liang Hanjing, director of financial technology at Invest Hong Kong, said at the Web3 closed-door meeting on June 12 that Hong Kong's proposal to build a Web3 center is not essentially about the securitization of virtual product assets, but about introducing Hong Kong's future economic and social transformation. This shows the significance of Web3 to Hong Kong. Hong Kong's friendly attitude towards Web3 is expected to attract a large number of builders who are bound by regulations to open up a new world in Hong Kong.

10. The SEC's battle with the crypto community

On June 5, SEC sued Binance, Binance US, and CEO Changpeng Zhao for allegedly violating federal securities laws by illegally offering and selling securities to U.S. investors. In this document, various crypto assets including but not limited to BNB, BUSD, SOL, ADA, MATIC, FIL, ATOM, SAND, MANA, ALGO, AXS, and COTI are listed as securities. This is another pressure from the U.S. regulators after Binance and its CEO were prosecuted by the Commodity Futures Trading Commission (CFTC) on March 28 this year for allegedly violating trading and derivatives rules.

The regulation is not just for Binance. SEC also sued Coinbase the next day, claiming that Coinbase provided trading services of crypto assets which are listed as securities without ever registering as a broker, national stock exchange or clearinghouse.

As the crypto market grows, reasonable regulation is conducive to business compliance and the healthy development of the industry. Promulgating clear and appropriate rules is not only the responsibility of regulators, but also the appeal of practitioners in the encryption industry. Only when the rules are clear, will more funds enter the market. However, the SEC's delay in releasing an unclear rulebook has opened up multiple rounds of litigation, turning the encryption market upside down. In addition, the U.S. regulatory level has not yet reached a unified opinion. The SEC and CFTC have issued contradictory statements to compete for the management of cryptocurrencies.

According to Zippia, about 44.3 million people in the United States hold cryptocurrencies, accounting for 13.22% of the total population, making it a country with a high acceptance of cryptocurrencies. The SEC's recent raid on the crypto community prompted some market makers to sell altcoins, resulting in a sharp drop in market liquidity and heavy losses for investors. Regulators should take both regulatory and development functions into account. It is lazy and irresponsible to blindly apply the old regulatory system to innovative assets. From this, we can foresee that Web3 builders originally in the United States will consider relocating to more crypto-friendly countries and regions due to regulatory pressure.

We need to be clear that tokenization is not to evade securities laws. It is a product of the demand for blockchain technology in practical applications and it is an improvement on the traditional organizational systems. The decentralized nature of blockchain makes it more resilient to attacks than any centralized system. The completely opposite regulatory attitudes of the United States and Hong Kong make us think that this may be the beginning of the rise of the east and the fall of the west in the Web3 space.

III.
Summary of Global Virtual Asset Regulatory Policies in H1 2023

This chapter was written by Will Liao @Legal Dao
http://liaowang@dehenglaw.com

1. Hong Kong launched a new regime for Virtual Asset Service Provider (VASP)

With the introduction of the "Policy Statement on Virtual Asset Development in Hong Kong" in October last year, the new VASP regime for virtual assets in Hong Kong [1] has come into effect on June 1, 2023, which is a major boon to the virtual asset industry in Hong Kong, China.

As early as 2018, the Hong Kong Securities and Futures Commission (SFC) gradually established a set of "voluntary licensing" system for the virtual assets of security tokens, which clearly stipulates that SFC does not have the authority to regulate virtual asset trading platforms that only buy and sell non-security tokens. Under the "voluntary licensing" regime, virtual asset trading platforms that are engaged in non-securities-based tokens do not need to be licensed.

Today, the virtual asset industry has undergone a dramatic transformation, and the original "voluntary licensing" system is no longer able to cover a market dominated by retail investors and non-security tokens. In order to comprehensively regulate all centralized virtual asset trading platforms in Hong Kong and implement the latest standards of the Financial Action Task Force (FATF), the Hong Kong government has revised the Anti-Money Laundering Ordinance and established a new VASP "mandatory licensing" system, with the aim of achieving a more appropriate balance between investor protection and market development.

Upon formal implementation of the VASP regime, all centralized virtual asset exchanges operating in Hong Kong or actively promoting their services to Hong Kong, whether or not they offer securities-based token trading services, will be required to be licensed and regulated by SFC.

SFC will implement measures in the second half of the year to allow licensed virtual asset exchanges to provide services to retail investors, but only tokens that are non-securities and have high liquidity in one of the traditional financial indices will be allowed to be provided to retail investors.

The regulatory arrangements for stablecoins will be implemented in 2023/24, and a licensing and permitting system for related activities will be established. Before stablecoin is regulated, SFC believes that stablecoins should not be included for retail trading.

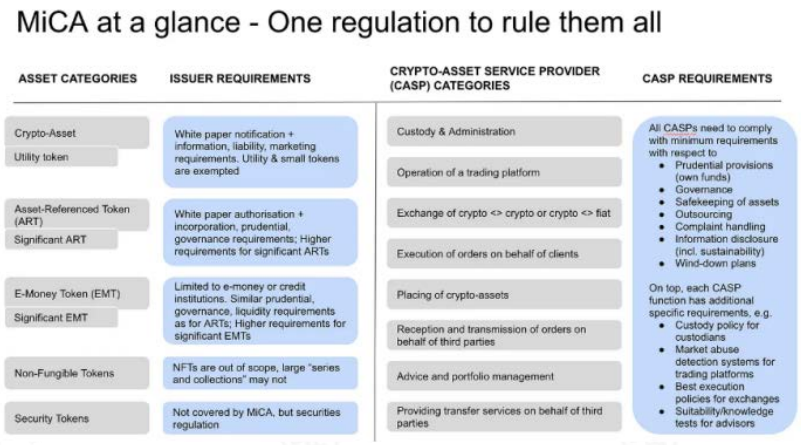
2. The European Union released the Markets in Crypto-Assets (MiCA) act

The Markets in Crypto-Assets (MiCA) was enacted by the European Union on May 31 and published in the Official Journal of the European Union (OJEU) on June 9 [2]. The MiCA will be implemented on December 30, 2024, after an 18-month transition period.

MiCA is part of EU's macro-level Digital Finance Strategy package, which will harmonize the following rules across EU member states: transparency and disclosure requirements for access to crypto-asset issuance and trading; authorization and regulation of crypto-asset service providers and issuers; rules for the operation, organization and governance of Asset-Referenced Tokens (ARTs), Electronic-Money Tokens (EMTs) and other crypto-asset service providers; rules for the protection of crypto-asset consumers; measures to prevent market abuse and ensure the integrity of the crypto-asset market.

MiCA fills the gap in the current EU financial regulatory framework by establishing a virtual asset regulatory framework that applies to all entities involved in the Issuance of Crypto-Assets in the EU and providing virtual asset-related services. In general, MiCA regulates: (i) all types of Crypto-Assets, including E-Money Tokens, Asset-Referenced Tokens and other Tokens; (ii) various Crypto-Asset Services and Service Providers, including wallet custody services, deposit and withdrawal services, exchange services, asset management services, investment advisory services, etc.

(from EU Markets in Crypto–Assets (MiCA) Regulation Expected to Enter into Force in Early 2023, Mayer Brown)



(from：https://paddihansen.substack.com/p/the–eus–mica–framework)

3. The UK House of Lords passed the Virtual Currency and Stablecoin Regulation Act

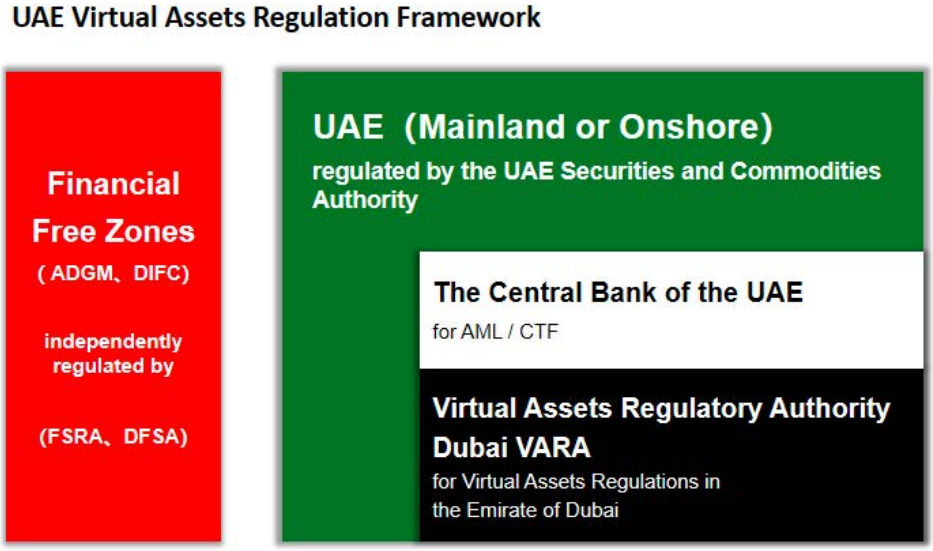
Following the enactment of MiCA, UK's virtual asset regulation legislation is catching up. The UK House of Lords reportedly voted to pass the Financial Services and Markets Bill (FSMB) on June 19 [3], meaning that the bill will enter the final stage before being signed into law, and the UK is likely to see a formal FSMB regulating virtual assets in the near future.

The bill treats virtual assets as a regulated activity, starting with regulating some stablecoins as a payment method. The bill proposes to extend the application of Part 5 of the Banking Act of 2009 to include payment systems using digital settlement assets. This would put the promotion of certain stablecoins within the purview of the Financial Conduct Authority (FCA).

Additionally, the bill will also give government regulators powers to create new regulated virtual assets and activities to fit within the current framework of traditional financial regulation. Currently, the FCA only has the power to ensure that virtual asset companies are registered with it and comply with its anti-money laundering rules. The bill also seeks to enhance coordination among regulators on new technologies, data usage, and decentralized technologies such as virtual currencies, stablecoins, NFTs, tokenization, and blockchain.

4. 2023 Virtual Assets and Related Activities Regulation (VARA Regulation) issued by the UAE

On February 7, 2023, the Dubai Virtual Assets Regulatory Authority (VARA) issued the Virtual Assets and Related Activities Regulations 2023 (VARAR)[4] which, with immediate effect, require all market participants (other than the two Financial Free Zones ADGM, DIFC) conducting virtual asset business or providing services in the UAE to be approved and licensed by the Emirates Securities & Commodities Authority (SCA) or VARA.



The VARA Regulations were issued under the Emirate of Dubai Virtual Assets Regulation Law No. [4] of 2022, which previously established the Dubai Virtual Assets Regulatory Authority (VARA) as the world's first independent governmental virtual assets regulator. This will create a robust regulatory framework for the governance of virtual assets and blockchain technology in Dubai.

The VARA regulations confirm the authority of VARA to issue rules, directives or guidelines regarding virtual asset activities. Subjects planning to conduct virtual asset activities in Dubai need to obtain a license from VARA prior to conducting such activities. These activities includes advisory services, broker-dealer services, custody services, trading services, lending services, payment and remittance services, and management and investment services for virtual assets. In addition, VARA also regulates (1) the classification and licensing of virtual assets; (2) compulsory registration of large-scale dealers; (3) Rules for the activities of virtual asset service providers; (4) Anti-money laundering; (5) marketing and promotion; (6) market violations; and (7) fines and penalties.

In addition, the UAE Central Bank issued new Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) guidelines for licensed financial institutions on May 31 [5] to help relevant institutions understand the risks posed by virtual assets and their service providers. The new guidance is based on the Financial Action Task Force (FATF) standards and will be implemented within a month. It is intended for banks, financial companies, exchanges, payment service providers, money transfer services, insurance companies, agents and brokers, etc.

It is reported that virtual asset exchange OKX Middle East has been granted a Minimum Viable Product (MVP) pre-license by the VARA in Dubai, OKX says that once MVP license is fully operational, OKX Middle East will offer spot, derivatives and fiat currency services, including USD and AED deposits, withdrawals and spot pair transactions [6].

5. Korea passed the Virtual Asset Investor Protection Act

The Korean National Assembly has reportedly passed the first phase of the virtual asset bill, the Virtual Asset Investor Protection Act, on May 11. The core of the first phase of virtual asset legislation is the introduction of protecting legal rules such as protecting customer assets and eliminating unfair trading. The second phase of the country's legislation will advance additional regulations for market order such as virtual asset issuance and disclosure while international standards for virtual assets are introduced [7].

The bill regulates the virtual asset market, unifying the terms cryptocurrency, crypto asset and digital asset as "virtual asset", which is defined as "an electronic token that has economic value and is capable of being traded or transferred", while central bank digital currency (CBDC) is excluded from virtual assets. The bill will also allow users to claim compensation for unfair trading of virtual assets. At the same time, unfair trading using undisclosed information, market price manipulation, and illegal trading will be punishable by fines. The basic penalty for unfair trading is imprisonment for more than one year or a fine of up to five times the amount of the unfair gain, and the penalty may be increased according to the amount of profit or loss.

Through the bill, the Financial Supervisory Commission (FSC) of Korea has the authority to supervise and examine virtual asset operators, and the National Assembly of Korea can also establish a virtual asset committee to be responsible for consultation on virtual assets. In addition, the second phase of legislation regarding the promotion of virtual asset issuance and disclosure of market information will be enacted at a later date. Baek Hye Ryun, chairman of the National Assembly Political Affairs Committee, said, "Virtual assets have finally entered the scope of the law."

6. Japan's largest bank is in talks to issue a global stablecoin

Mitsubishi UFJ Financial Group, Japan's largest bank, is reportedly in talks with global stablecoin issuers and other companies about issuing its stablecoin. Tatsuya Saito, vice president of products at Mitsubishi UFJ, said the bank is in discussions with multiple parties to use its blockchain platform Progmat to issue stablecoins pegged to foreign currencies, including the U.S. dollar, for global use. He said issuers and users would feel safe using stablecoins since Japanese legislation is in effect. However, he declined to say which stablecoin parties he was negotiating with.

In June 2022, Japan passed an amendment to the world's first stablecoin bill, the Fund Resolution Act, which classifies stablecoins as virtual currencies and allows licensed banks, registered transfer agents, and trust companies to act as issuers of stablecoins. in December 2022, Japan's financial regulator removed the prohibition on overseas stablecoins trading. Stablecoins, which are somewhat in between fiat currencies and virtual currencies, are considered to be a key part of the development of Web3. Stablecoins can be pegged to the Japanese yen, and people in Japan can purchase various tokens through them.

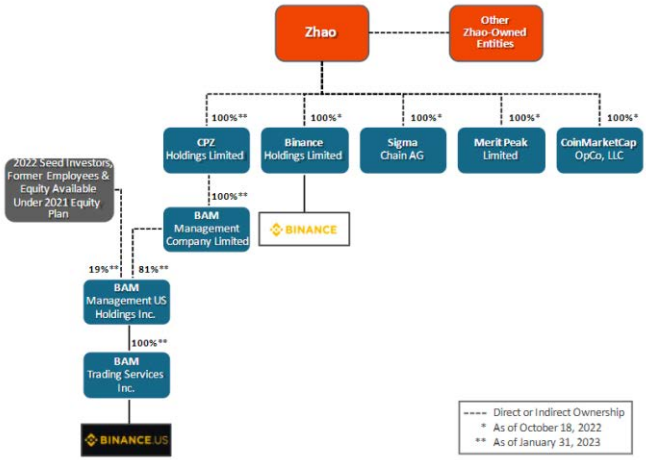
7. Crypto-friendly banks Slivergate Bank and Signature Bank were taken over by FDIC

On March 1, 2023, Silvergate Bank issued an announcement that it would not be able to file its annual 10-K report with the SEC on time and stated that it may be "undercapitalized. Silvergate Bank is a California-based community retail bank that has positioned itself as a gateway to the virtual asset industry, accepting deposits from virtual asset exchanges and institutions, and has established its own virtual currency settlement payment network, the Silvergate Exchange Network (SEN) real-time payment system. This system enables virtual asset exchanges, institutions and customers to exchange virtual currency for fiat currency.

The collapse of FTX in November 2022 left Silvergate Bank with over $1 billion of exposure to FTX. More seriously, the collapse of FTX caused a severe "bank run," with Silvergate Bank processing over $8.1 billion in withdrawals, and in order to meet the large withdrawals, Silvergate Bank was forced to suffer large discount losses and urgently sell approximately $5.2 billion in assets and obtain a $4.3 billion loan from the Federal Home Loan Bank. On March 8, 2023, Silvergate Bank stated in a filing to the SEC that it would wind down its operations and voluntarily liquidate Silvergate Bank in accordance with applicable regulatory procedures. "The Bank's liquidation plan includes the full repayment of all deposits and how to best resolve claims while retain the residual value of its assets, including its proprietary technology and tax assets." Subsequently, Silvergate Bank was taken over by the Federal Deposit Insurance Corporation (FDIC).

On March 10, 2023, against the backdrop of a Fed rate hike, a brief 48-hour bank run caused Silicon Valley Bank (SVB), the 16th largest bank in the U.S. with a 40-year history, to suffer severe liquidity problems and be taken over by the FDIC. On March 12, 2023, the Treasury Department, the Federal Reserve, and the FDIC issued a joint statement indicating that they had agreed, after consultation, to complete their bailout of Silicon Valley Bank through the FDIC in a manner that fully protected all depositors. Starting from Monday, March 13, depositors will be able to access and withdraw all their funds, and any losses related to the resolution of Silicon Valley Bank will not be borne by taxpayers.

As a result of the impact of Silicon Valley Bank, on March 12, 2023, the U.S. Treasury Department, the Federal Reserve Board, and the FDIC issued a joint statement announcing the closure of Signature Bank, a crypto-friendly bank, citing "systemic risk" to prevent the banking crisis from spreading [8]; at the same time, NYDFS appointed the FDIC as receiver to dispose of Signature Bank's assets, even though Signature Bank had recovered from the effects of Silicon Valley Bank and had a strong balance sheet.



(from Crypto's Last Stand in the US: USDC, Silvergate, Silicon Valley and Signature Banks Collapse in One Week)

8. US regulatory enforcement against Binance and its founder CZ

8.1 New York financial regulator asks Paxos to stop raising its stablecoin BUSD

On February 13, 2023, Binance CZ issued a statement that the New York State Department of Financial Services (NYDFS) has instructed stablecoin issuer Paxos to stop minting new BUSD, a stablecoin wholly owned and managed by Paxos. At the same time, Paxos confirmed that it has received notice from the SEC regarding potential charges related to its BUSD product.

Paxos is a New York State-registered stablecoin issuer that holds a New York State Bitlicense, a virtual asset operating license that directly regulated by NYDFS, and its BUSD product is built on the Ethereum blockchain and fully reserved at 1:1 USD assets as required by NYDFS's USD stablecoin issuance guidelines issued in June 2022. NYDFS states that this regulatory initiative is intended to clarify unresolved complex issues between Paxos and Binance.

Paxos responded to NYDFS' regulatory initiative via its website, stating that it will cease the issuance of new BUSD tokens in accordance with NYDFS's instructions and work closely with the agency since February 21. Paxos will terminate its partnership with Binance regarding BUSD and will introduce Pax Dollar (USDP) as a replacement for the previous BUSD. [9]. NYDFS subsequently clarified more in a report with Bloomberg [10]. The reason for NYDFS' request does not seem to be related to the securities designation of the stablecoin; the real reason may be related to Circle's complaint about the mismanagement of Binance-Peg BUSD's reserves.

8.2 CFTC charges Binance and its founder CZ of deliberately evading U.S. law to operate an illegal virtual asset derivatives exchange

On March 27, 2023, the US Commodity Futures Trading Commission (CFTC) announced that it had filed a civil lawsuit in US court accusing CZ and three entities operating the Binance platform of repeatedly violating the Commodity Exchange Act (CEA) and CFTC regulations [11]. According to the complaint, from July 2019 to present, Binance offered and executed virtual asset derivatives transactions to U.S. persons (despite shielding U.S. IP addresses), and at CZ's direction, Binance instructed its employees and clients to deliberately evade U.S. law by circumventing compliance controls (including through VPNs, setting up shell companies, etc.), conducting business in an opaque manner, and ignoring CEA and CFTC regulations, while systematically engaging in regulatory arbitrage for commercial gain [12].

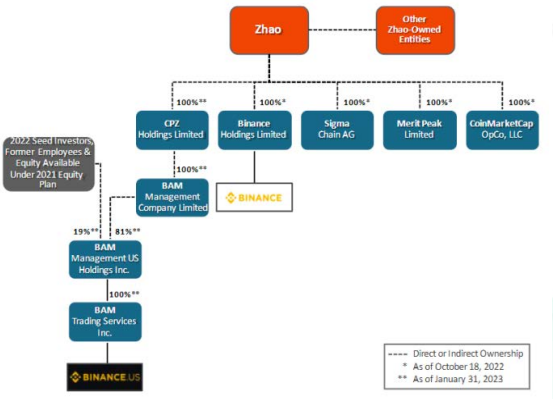
The CFTC alleges that entities such as Binance that provide derivatives services on virtual assets in the United States should register with the CFTC as Futures Commission Merchants (FCMs) to undertake compliance obligations similar to KYC and to implement basic compliance requirements designed to prevent and detect terrorist financing and money laundering activities. According to the derivatives trading operations carried out by Binance, it should also be registered with the CFTC as a Designated Contract Market (DCM) or Swap Execution Facility (SEF). Binance has never had any registration with the CFTC.

As such, CFTC has charged CZ and related parties through a civil lawsuit with violating various laws and regulations related to futures trading, illegal off-exchange commodity options, failure to register as a futures commission merchant, or designated contract market, or swap execution facility, as well as lax supervision, failure to implement KYC or AML processes, and the creation of inadequate compliance programs. The CFTC is seeking civil penalties and permanent trading and registration bans against CZ and related parties through the court.

CFTC Chairman Rostin Behnam said, "Today's enforcement action demonstrates that no jurisdiction, or jurisdiction that claims not to have jurisdiction, can prevent the CFTC from protecting U.S. investors. I have made it clear that the CFTC will continue to use all of its powers to uncover and stop improper conduct in the volatile and high-risk virtual asset industry...- For years, Binance has knowingly flouted CFTC regulations while actively operating to maintain cash flows and avoid compliance. This should serve as a warning to everyone in the virtual asset world that the CFTC will not tolerate intentional evasion of U.S. laws."

8.3 SEC files 13 charges against various entities including Binance and its founder CZ

On June 5, 2023, the SEC filed 13 charges against various entities, including Binance and its founder CZ, for operating unregistered exchanges, broker-dealers, and clearing agencies; engaging in fraudulent trading and ineffective regulation of Binance US; and issuing and selling unregistered securities [13].



This enforcement action follows a similar action brought against Binance by the CFTC in March. In a 136-page indictment [14], the SEC charged CZ and various entities, including Binance, with multiple dimensions: Binance's unlawful solicitation of U.S. investors to buy, sell, and trade virtual currencies and failure to restrict U.S. investors' access to Binance.com; Binance's unregistered offering and sale of securities, including BNB, BUSD and loan products known as "Simple Earn" and "BNB Vault," as well as so-called pledged investment programs offered on Binance. SEC also noted that Binance secretly controlled the pledges made by U.S. customers in the BAM pledge program; that various entities, including Binance, repeatedly misled investors by allowing them to commingle customer assets or transfer customer assets at will, including to the Merit Peak Limited entity, which CZ effectively controlled, echoing similar allegations made by FTX and its founder Sam; that various entities, including Binance, should have been registered as stock exchanges, broker-dealers, and clearing houses; US lied about preventing market manipulation and allowed an undisclosed "market maker" trading firm, Sigma Chain, also owned by CZ, to engage in Washing Trading.

SEC Chairman Gary Gensler slammed CZ and various entities such as Binance for "creating a network of massive deception, conflicts of interest, lack of disclosure, and intentional evasion of the law. "As alleged, CZ and various entities such as Binance misled investors about their risk controls and false trading volumes, while actively concealing the platform operators, manipulating their affiliated market makers to trade, and even using funds held in custody by investors," Gensler said in a press release: "They sought to evade U.S. securities laws through false controls so they could keep high-value U.S. customers on their platforms. The public should beware of investing any of their hard-earned assets in or on these illegal platforms."

In addition to the allegations against Binance, the virtual currencies listed as securities in the lawsuit filing include but are not limited to, BNB, BUSD, SOL, ADA, MATIC, FIL, ATOM, SAND, MANA, ALGO, AXS, COTI. The SEC emphasizes that the tokens listed are "including, but not limited to The SEC emphasizes that the tokens listed are". It is worth noting that ETH, USDC, USDT, LTC and other tokens with large trading volumes are not included. Previously, the SEC chairman has stated that any virtual currency other than Bitcoin may contain securities properties.

9. SEC's Regulatory Enforcement of Coinbase, the Largest U.S. Listed Compliance Exchange

No more than one day after SEC sued Binance and CZ, SEC filed another lawsuit against Coinbase, the nation's largest virtual asset compliance exchange, on June 6. This lawsuit differs from SEC's lawsuit against Binance and CZ in that it reflects more on the regulatory challenges and legal compliance framework that virtual asset exchanges need to face[15].

Coinbase became the first integrated financial services provider for virtual assets to go public in the U.S. in April 2021, and is known for its compliance, holding a New York State BitLicense and Trust license, MTL licenses in every state in the U.S., as well as a UK FCA and Irish Central Bank license for electronic money services, offering a wide range of virtual asset services such as fiat money deposit and withdrawal and coin-currency trading. The company is also licensed by the UK FCA and the Irish Central Bank for electronic money services.

According to the SEC's allegations [16], Coinbase integrated the traditional financial services of exchanges, brokers, and clearing agencies. Because the subject matter of the transactions included Crypto Asset Securities, they were then required by law to register with the SEC. As a result, Coinbase's violations included (1) unregistered brokers, including soliciting potential investors, handling customer funds and assets, and charging transaction fees; (2) unregistered exchanges, including providing a marketplace that brings together multiple buyers and sellers of virtual assets for order matching and execution; and (3) unregistered clearing agencies, including holding customer assets in wallets controlled by Coinbase, and collecting transaction fees through debits.

SEC also charged Coinbase with offering and selling unregistered securities to customers through its pledge product (Staking-as-a-Service Program). The Staking-as-a-Service Program offers users a pledged product of underlying tokens with an income return by escrowing their assets. The SEC took regulatory enforcement action against San Francisco-based virtual asset exchange Kraken in February of this year for the same reason, and Kraken ultimately agreed to pay tSEC $30 million and cease offering its Staking-a-Service product to U.S. customers to settle the SEC's charges of offering unregistered securities.

In addition, SEC has classified 13 tokens on the Coinbase platform as security-based tokens, including SOL, ADA, MATIC, FIL, SAND, AXS, CHZ, FLOW, ICP, NEAR, VGX, Dash, NEXO, and notably the SEC notes that this is a Non-Exhaustive List .

10. U.S. regulators actively explore regulatory paths for DeFi

On April 6, 2023, the U.S. Treasury Department released the 2023 DeFi Illicit Financial Activities Assessment [17], the world's first DeFi-based assessment of illicit financial activities and a response to the White House's virtual asset regulatory framework released in March 2022. Both FinCEN, a division of the U.S. Department of the Treasury, and OFAC, the Office of Foreign Assets Control, are key regulators of the U.S. virtual asset industry. FinCEN is responsible for preventing and punishing domestic and international money laundering activities, combating terrorist financing and other financial crimes, as well as collecting and analyzing financial transaction information. While OFAC is responsible for administering and enforcing all economic and trade sanctions based on U.S. national security and foreign policy.

The report begins with an overview of the market structure of the DeFi ecosystem, where DeFi services are broadly defined as DeFi platforms, exchanges, applications, organizations, and other forms of decentralized exchanges (DEX), decentralized lending platforms, pledge pools (Yield Protocols), cross-chain bridges, liquidity pledges, decentralized algorithmic stablecoins, and more. But it does not include DeFi services for transactions between self-hosted wallets. The report then notes that in practice most so-called DeFi is still centralized, often controlled by an organization that provides a degree of centralized management and governance. The report demonstrates how illicit actors misuse DeFi services to engage in and profit from illegal activities, specifically ransomware attacks, theft, fraud, drug trafficking, and proliferation financing. In addition, the report identifies vulnerabilities in DeFi services that can be used by criminals for illicit financial conduct, including non-compliance with anti-money laundering/counter-terrorism financing (AML/CFT) and sanctions obligations, the risk of disintermediation, and the regulatory vacuum of lack of compliance with international AML/CFT standards in overseas jurisdictions. Finally, the report recommends that the U.S. strengthen AML/CFT regulation and, where possible, enforcement of virtual asset activities, including DeFi services, to improve compliance with BSA obligations by virtual asset service providers.

11. SEC's regulation of virtual asset custody leads to the entry of Wall Street capital

On February 15, 2023, the SEC issued a proposal for Qualified Custodians for Investment Advisers that further increases the custody requirements for virtual assets and extends the requirements to investment advisers such as funds, requiring them to use Qualified Custodians to hold the underlying virtual assets[18].

In particular, SEC Chairman Gary Gensler emphasized that the regulations currently in place (the 2009 regulations) were able to cover and subject a significant amount of virtual assets to regulation. While some virtual asset trading and lending platforms claim to be able to hold investors' virtual assets in custody, this does not mean that they are qualified custodians, and some platforms do not properly segregate investors' virtual assets, but instead commingle investors' assets, resulting in a "bank run" or similar situation where investors' assets became the assets of the failed company. This is a serious violation of investors' interests. With this expanded regulation, both investors and investment advisors will receive the protection they deserve.

In his August 2022 working video "What Are Crypto Trading Platforms?"[19], Gary Gensler discusses SEC's thinking on the regulation of virtual asset markets: (1) Building on the well-functioning U.S. Securities Act, which has been in operation for 90 years, to protect the interests of investors; (2) It is necessary to split virtual asset exchanges (such as splitting brokerage, clearing and settlement, and custodial businesses) to avoid conflicts of interest and self-dealing.

REFERENCE:

[1] Consultation Conclusions on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed by the Securities and Futures Commission
https://apps.sfc.hk/edistributionWeb/api/consultation/conclusion?lang=EN&refNo=23CP1

[2] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

[3] UK https://bills.parliament.uk/ Financial Services and Markets Bill
https://bills.parliament.uk/bills/3326

[4] VARA, Virtual Assets and Related Activities Regulations 2023
https://www.vara.ae/en/regulations/regulations-and-guidelines/

[5] UAE central bank issues AML/CTF guidance for dealing with virtual assets
https://www.reuters.com/technology/uae-central-bank-issues-amlctf-guidance-dealing-with-virtual-assets-2023-05-31/

[6] Crypto Exchange OKX Wins Preparatory License in Dubai, Set to Boost Staff
https://www.coindesk.com/business/2023/06/15/crypto-exchange-okx-wins-preparatory-license-in-dubai-set-to-boost-staff/

[7] Protection of virtual asset investors in Korea and obligations imposed on virtual asset service providers
https://www.lexology.com/library/detail.aspx?g=2c2f8d35-9dac-4921-ad10-500eb2f40572

[8] Signature Bank, Joint Statement by the Department of the Treasury, Federal Reserve, and FDIC
https://www.fdic.gov/news/press-releases/2023/pr23017.html

[9] Paxos Issues Statement
https://paxos.com/2023/02/13/paxos-issues-statement/

[10] Bloomberg, Stablecoin Issuer Circle Warned Watchdog About Binance Token
https://news.bloomberglaw.com/securities-law/stablecoin-issuer-circle-warned-ny-watchdog-about-binance-token

[11] CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange
https://www.cftc.gov/PressRoom/PressReleases/8680-23

[12] Commodity Futures Trading Commission v. Zhao et al
https://www.courtlistener.com/docket/67092867/1/commodity-futures-trading-commission-v-zhao/

[13] SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao
https://www.sec.gov/news/press-release/2023-101

[14] SECURITIES AND EXCHANGE COMMISSION v. BINANCE HOLDINGS LIMITED, 1:23-cv-01599, (D.D.C.)
https://www.docdroid.net/l02zzqT/sec-v-binance-4-pdf

[15] SEC Charges Coinbase for Operating as an Unregistered Securities Exchange, Broker, and Clearing Agency
https://www.sec.gov/news/press-release/2023-102

[16] Securities and Exchange Commission v. Coinbase, Inc., 1:23-cv-04738, (S.D.N.Y.)
https://www.sec.gov/litigation/complaints/2023/comp-pr2023-102.pdf

[17] Treasury Releases 2023 DeFi Illicit Finance Risk Assessment
https://home.treasury.gov/news/press-releases/jy1391

[18] SEC Proposes Enhanced Safeguarding Rule for Registered Investment Advisers
https://www.sec.gov/news/press-release/2023-30

[19] Office Hours with Gary Gensler: What Are Crypto Trading Platforms?
https://www.sec.gov/news/sec-videos/office-hours-gary-gensler-what-are-crypto-trading-platforms

IV.
Web3 in Africa & MENA: A Review of Adoption, Incubation, and Security Breaches

This chapter was written by SOUHAIL MSSASSI – AMJAD KOUBRI – SOUFIANE AMOUGAI @ShellBoxes

Blockchain technology has emerged as a disruptive force with the potential to revolutionize various sectors across Africa and the MENA region. This report presents an in-depth analysis of the adoption and progress of blockchain technology in selected African and MENA countries, shedding light on the regulatory frameworks, use cases, and transformative impact of blockchain in different sectors.

1. Blockchain Adoption in African Countries:

South Africa: South Africa has embraced blockchain technology and recognizes its potential for economic growth and financial inclusion. The South African Reserve Bank has conducted pilots to explore the use of blockchain for interbank settlement. Additionally, initiatives such as the South African Blockchain Alliance and Project Khokha have driven advancements in areas like supply chain management, identity verification, and remittances.

Kenya: Kenya has emerged as a leader in blockchain adoption, particularly in the areas of finance and agriculture. The government has set up the Blockchain and Artificial Intelligence Taskforce to explore the potential of these technologies. In the agricultural sector, blockchain-based platforms like Farm to Market Alliance and Twiga Foods have facilitated transparency, traceability, and access to finance for farmers.

Tunisia: Tunisia has made notable progress in blockchain adoption, focusing on financial inclusion and government services. The country launched its national currency, the eDinar, on the blockchain to cater to the unbanked population. The Tunisia Economic City (TEC) project is also partnering with the Locus Chain Foundation to apply blockchain technology as a settlement currency and service platform.

Mauritius: Mauritius has emerged as a frontrunner in the adoption of blockchain technology in Africa. The government's proactive approach in establishing a robust regulatory framework has positioned the country as a leading blockchain and fintech hub. The Financial Services Commission (FSC) plays a pivotal role in overseeing and licensing digital asset custodian services, fostering innovation within the sector.

Nigeria: Nigeria has witnessed a surge in blockchain adoption, driven by the emergence of native blockchain companies. Despite the Central Bank of Nigeria's prohibition on financial institutions engaging in cryptocurrency-related activities, Nigeria has become one of the largest holders of bitcoin globally, reflecting the country's interest in decentralized digital assets.

South Africa: South Africa's regulatory approach to cryptocurrencies is nuanced, with the South African Reserve Bank (SARB) engaging in fintech initiatives to explore distributed ledger technologies (DLTs). Project Khokha, a successful pilot project conducted by SARB, demonstrated the feasibility of using DLTs for interbank settlement. The South African Revenue Service (SARS) classifies cryptocurrencies as assets and imposes tax regulations accordingly.

Senegal: Senegal has made significant strides in digital currency adoption through the introduction of the eCFA, a national digital currency. Regulated by the Banque Regionale de Marches (BRM) and eCurrency Mint, the eCFA aims to enhance financial inclusion, interoperability, and transparency within the West African Economy and Monetary Union (WAEMU).

Sierra Leone: Sierra Leone has demonstrated pioneering efforts by utilizing blockchain technology in its national election process. The adoption of the Agora platform, a blockchain-based digital voting solution, enhanced transparency and minimized election disputes. Sierra Leone's plan to implement a national identification system using distributed ledger technologies will improve personal data security and access to financial services for the unbanked population.

Democratic Republic of the Congo (DRC): The DRC has witnessed the pilot implementation of a blockchain-based supply chain tracking system for cobalt and coltan mining. This system, initiated by Dorae Inc., ensures traceability and transparency in the supply chain, providing end users with reliable information about the source of raw materials. By combating child labor and environmentally damaging mining practices, the DRC aims to promote sustainable and ethical mining.

Madagascar: Madagascar has harnessed blockchain technology for conservation projects through a partnership between the Ixo Foundation and the Seneca Park Zoo. The use of blockchain enables transparent monitoring and recording of tree-planting efforts in conservation areas. By providing verified impact data, this initiative enhances donor confidence and supports sustainable social, environmental, and economic development.

Ethiopia: Ethiopia has taken steps towards blockchain adoption by collaborating with Cardano, a cryptocurrency start-up, to establish a blockchain-based supply chain application for coffee shipments. By leveraging blockchain technology, Ethiopia aims to ensure transparency, quality assurance, and fair trade practices within its coffee industry.

2. Blockchain Adoption in MENA Countries:

Bahrain: Bahrain has positioned itself as a leading blockchain hub in the MENA region, with a regulatory sandbox that encourages blockchain experimentation. The Central Bank of Bahrain has introduced regulations governing cryptocurrencies and initial coin offerings. Bahrain's blockchain strategy aims to foster adoption in sectors such as finance, healthcare, and logistics.

United Arab Emirates (UAE): The UAE has been at the forefront of blockchain adoption, integrating the technology into government services. The Dubai Blockchain Strategy and the Emirates Blockchain Strategy have driven advancements in areas like identity management, supply chain, and smart cities. The Dubai International Financial Centre (DIFC) has established a comprehensive regulatory framework for digital assets.

Saudi Arabia: Saudi Arabia recognizes the potential of blockchain technology and has implemented various initiatives to harness its benefits. The Saudi Arabian Monetary Authority has collaborated with Ripple to pilot blockchain solutions for cross-border payments. The Saudi Blockchain Strategy focuses on sectors such as government services, healthcare, and finance.

Qatar: Qatar has made notable strides in blockchain adoption, particularly in the finance and logistics sectors. The Qatar Financial Centre has launched the Blockchain Sandbox initiative to facilitate testing of blockchain-based solutions. The country's initiatives aim to enhance supply chain transparency, land registration, and digital identity verification.

Egypt: Egypt has recognized the potential of blockchain technology in driving financial inclusion and efficiency. The country has established entities such as the National Blockchain Council and the Egyptian Blockchain Technology Innovation Cluster. Use cases in Egypt include digital identity, supply chain management, and land registry.

Jordan: Jordan has embarked on blockchain initiatives to enhance government services and foster innovation. The Jordanian government has collaborated with the International Finance Corporation on the use of blockchain for supply chain finance. Blockchain-based solutions have been explored for areas such as trade finance, energy, and healthcare.

Comparative Analysis and Conclusion:

The adoption of blockchain technology in African and MENA countries varies, with each country demonstrating unique strengths and initiatives. While African countries like South Africa and Kenya have focused on financial inclusion and supply chain management, MENA countries like Bahrain and the UAE have leveraged blockchain for government services and smart city initiatives. These regions have recognized the transformative potential of blockchain in sectors such as finance, agriculture, logistics, and identity management.

It is essential for policymakers and stakeholders in both regions to continue fostering supportive regulatory frameworks, collaboration between public and private sectors, and capacity building to unlock the full potential of blockchain technology. Further research and analysis are recommended to monitor the progress and assess the long-term impact of blockchain adoption in Africa and the MENA region.

3. Web3 startups Evolution in MENA

What is the level of adoption of blockchain and cryptocurrency in Africa? Well, based on the previous section the response is varied. Although the private sector is rapidly adopting these technologies in many countries, governments have been hesitant and cautious, and in some cases, unenthusiastic. Zimbabwe and Namibia, for instance, have reportedly taken a tough stance, while Mauritius is leading the way in the region. The progressive attitude towards the potential economic benefits of cryptocurrencies is demonstrated by the regulatory sandbox established in Mauritius, which suggests that African countries can introduce regulations for blockchain and cryptocurrency while encouraging foreign direct investment through incentives. This presents a new opportunity for African nations to approach blockchain and cryptocurrency in a way that can benefit their economies. Throughout this report we will only scratch the surface and highlight a few promising blockchain based projects.

As a result of the regulatory relief observed in some regions of Africa, we can observe innovators throughout the continent integrating blockchain technology into their projects. Akon, a singer of African-American descent, has developed a strong interest in blockchain technology, which has inspired a remarkably audacious idea. He is currently working on a futuristic $6 billion project in Senegal, where he plans to build his own city. In this fantasy world, the Akoin cryptocurrency (AKN), which was officially launched in the cryptocurrency market in 2020, will be used as the primary method of payment. Akoin Utility Token is available within the Akoin Multi-Currency wallet for exchange between all DApp / App offerings and within the local market, including prepaid minute conversion (a major store of value in Africa), direct service payments (ie utility, mobile etc) and the ability to convert into local currency; all creating a strong value proposition for early adopters and users of the Akoin platform.

Moving on to Mauritius, The Mauritius Government is supportive of blockchain technology and initially implemented a sandbox license recognizing crypto currency as a digital asset. (Include citation) One prominent project is HABN, The Horizon Africa Blockchain Network (HABN) is a blockchain system based on Ethereum that offers a framework for blockchain solutions. In addition to this, the Horizon Africa initiative seeks to enhance the participation of African developers in the field of blockchain technology. The Horizon Africa blockchain Network will serve as a testing ground for creating and implementing basic or advanced Dapps (Decentralized Apps) that address issues unique to the African region, and enable Africa to communicate and collaborate more effectively with other nations.

Proceeding to Morocco, the latter took a definitive stance in 2017, by prohibiting the use and acceptance of cryptocurrencies. Despite the ban and the careful "wait and see" approach to digital currencies, there have been some minor yet notable developments in the technology underpinning cryptocurrencies, such as blockchain. For instance, Brookstone Partners, a private equity firm based in New York, has reportedly acquired a wind farm spanning 37,000 acres in Dakhla, Morocco, with the aim of using it to power a data center and mine bitcoin. The development of the wind farm will apparently be overseen by Soluna, a blockchain company with an environmentally-friendly focus, which plans to raise $100 million through an initial coin offering (ICO) to fund the project.

Zooming in on the middle east, Dubai is positioning itself as a leader in shaping the world's future economy, with a focus on innovation, technology, and forward-thinking policies. The Emirate is making progress on its D33 Agenda, which aims to establish Dubai as the capital of the Future Economy anchored by the Blockchain, Web3, AI, and the Metaverse. Dubai is investing heavily in building the necessary infrastructure and has established regulatory frameworks that support the needs of both domestic and international companies operating in the digital asset industry. The creation of the Virtual Assets Regulatory Authority (VARA) in 2022 has put Dubai at the forefront of global Crypto regulation, with clear and robust guidelines for Crypto asset businesses to follow. This supportive environment allows enterprises to thrive, create jobs, and increase economic growth while ensuring responsible behavior and protecting the interests of customers and investors.

The web3 ecosystem that is emerging in the Middle East is highly diverse, encompassing a broad range of components such as protocols, web3 infrastructure, DeFi, Crypto Exchanges, NFT platforms, Metaverse, and Web3 Gaming. This dynamic and multifaceted ecosystem is a testament to the region's ongoing commitment to innovation.

We can shed the light on BEEAH Group, which is a prominent sustainability leader in the region, with verticals spanning various industries. Known for innovative environmental practices and solutions for cities that are ready for the future, the company has invested in digital ventures that maximize technology's potential to create a positive impact on society. One such example is the development of Sharjah's first blockchain platform.

Additionally, Sheesha Finance is a top DeFi project and incubation hub that offers diversified cryptocurrency portfolios to investors of all sizes, from small to large. The company aims to become a member-managed Decentralized Autonomous Organization (DAO) and is committed to ensuring complete transparency and honesty within the DeFi industry. By providing a wide range of projects, Sheesha Finance rewards its investors with premium cryptocurrency portfolio diversification.

Regarding NFTs, The NFT industry in the Middle East is projected to experience an annual growth rate of around 45.5%, with a compounded annual growth rate of 32.1% from 2022 to 2028. In the past year, multiple NFT marketplaces have emerged in the UAE, making it more accessible for the public to engage in NFT trading. We can highlight NiftySouq, which is an NFT marketplace located in the MENA region that enables simple creation and trading of NFTs using fiat currencies such as AED and SAR. The platform places emphasis on large-scale projects, including sports, ticketing, music, and gaming NFTs, which are available in both Arabic and English.

4. Web3 Incubators in Africa/MENA

As blockchain technology is still in its embarkation phase in Africa, most tech hubs have not yet established a well-structured incubation and acceleration program to support community members working on blockchain solutions. Consequently, many of these innovators have turned to online communities for support and guidance. Web3 startups in Africa have reason to be optimistic as of late. The recently published African Blockchain Report 2022 by CV VC indicates that African blockchain technology startups are receiving increased funding. In fact, KuCoin, a cryptocurrency exchange based in Seychelles, received 33.8% of the total crypto and blockchain venture capital (VC) funding allocated to Africa in 2022. The report also highlights that Africa's blockchain funding growth rate was among the highest of all regions worldwide, indicating that the region is becoming an increasingly attractive destination for investors seeking blockchain-related opportunities.

Regarding the most prominent incubator hubs and venture capitalists in the region, we can identify:

Senex Group, a multinational conglomerate with operations in various industries, recently unveiled Nigeria's inaugural Web3 incubator hub to promote and expedite the growth and development of Web3 technologies in Nigeria and other regions. The launch ceremony was attended by renowned tech investors, influential entrepreneurs, key stakeholders from the public sector, and other important individuals.

EchoVC, a pan-African venture capital firm with a global footprint, has revealed a new $8 million fund that is specifically intended for blockchain startups operating in Africa. The fund, known as the EchoVC Chain Blockchain Fund, will be used to invest in startups that are developing practical blockchain solutions to address some of Africa's most pressing problems. This comes at a time when trust in cryptocurrency and blockchain startups is dwindling among customers and investors, making EchoVC's fund even more crucial to the growth and development of the industry.

Adaverse is a venture fund and accelerator supported by Cardano that aims to establish a strong foundation in Africa, Asia, and other regions. The initiative, which is a collaboration between EMURGO and Everest Ventures Group, brings together entrepreneurs, mentors, and strategists to support blockchain founders in scaling their Web 3 solutions through funding, mentorship, and technological infrastructure.Additionally, Emurgo Kepple Ventures is a partnership between Emurgo Africa and Kepple Africa Ventures, which seeks to offer investment-focused assistance to web3 startups in Africa.

CV VC and SECO have formed a partnership to embrace the rapidly developing African ecosystem, actively seeking out and engaging with the diverse talent and innovation that the continent has to offer. By combining the experience and expertise of Crypto Valley with a global network of partners and resources, our mission is to further accelerate the already fast-paced innovation and adoption of blockchain and cryptocurrencies in Africa. Since its inception, CV VC has achieved remarkable success, with African startups submitting more applications than those from any other region in the world.

The United Arab Emirates (UAE) is host to a wide variety of incubators, each with its particular strengths and areas of focus. In this section, we will illuminate some of the most notable incubators in the region:

Enhance Ventures is a pioneering venture studio in the MENAPT region (Middle East, North Africa, Pakistan, and Turkey), focused on developing and investing in ventures that shape the future of finance and commerce. In addition to building their ventures, they collaborate with corporations and government entities to create innovative ventures together. The company's innovative approach and commitment to fostering a culture of entrepreneurship have established them as a prominent player in the region's business landscape.

Crypto Oasis Ventures is a Web3 venture building company based in the Dubai International Financial Centre (DIFC), dedicated to nurturing the ecosystem and advancing blockchain-related organizations in the Middle East and beyond. As a trailblazer in the local blockchain venture building field, the company has established a global network, strengthened by its close links to Switzerland's Crypto Valley. Its portfolio of recent ventures includes Crypto Oasis Labs, Crypto Oasis Sentio, arte, Crypto Oasis Games Guild, and Inacta Communications.

The Dubai Blockchain Center was officially opened on May 14, 2018, by His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE, and Ruler of Dubai. The center's primary objective is to unite blockchain thought leaders, developers, investors, and educators from all over the world.

* This is not an exhaustive list

5. Enhancing Security in the Web3

Given the evolving threat landscape, web3 companies in Africa and globally should consider implementing the following measures:

a. Continuous Security Audits: Regular audits by reputable third-party firms to identify vulnerabilities and address them proactively.

b. Strong Authentication Mechanisms: Implementation of multifactor authentication and biometric verification to enhance user account security.

c. Employee Training and Awareness: Comprehensive cybersecurity training programs to educate employees about common attack vectors and best practices.

d. Incident Response Planning: Development of well-defined incident response plans to minimize damage, facilitate a swift recovery, and maintain trust among users.

e. Encryption and Secure Storage: Implementation of robust encryption protocols and secure storage mechanisms to protect sensitive user data and assets.

f. Collaboration and Information Sharing: Active participation in industry-wide initiatives, sharing threat intelligence, and collaborating with regulatory bodies to strengthen the overall security posture.

Motivations Behind Hacks in African Countries:

Understanding the motivations behind hacks in African countries can provide insights into the factors driving cybercriminal activities. While it is challenging to determine specific motivations without detailed information on individual cases, the following motivations are commonly observed:

a. Financial Gain: One of the primary motivations behind hacks in African countries, as well as globally, is financial gain. Hacker's target web3 companies in pursuit of assets such as cryptocurrencies, customer funds, or sensitive financial information. These assets can be monetized through various means, including selling them on the dark web or using them for fraudulent activities.

b. Lack of Security Awareness: The relatively nascent state of the web3 industry in Africa, coupled with limited cybersecurity awareness among businesses and users, presents an attractive target for hackers. Exploiting security vulnerabilities in web3 companies may be perceived as relatively easier compared to well-established organizations with robust security measures in place.

c. Political or Ideological Motivations: In some cases, hackers may have political or ideological motivations behind targeting web3 companies in African countries. This could involve actions aimed at disrupting the financial systems, highlighting perceived social or political injustices, or advancing specific agendas.

d. Insider Threats: Insider threats, where individuals with authorized access misuse their privileges for personal gain or malicious intent, can also contribute to breaches in African web3 companies. Insiders may exploit their knowledge of internal systems and processes to compromise security and access assets.

e. Reputation Damage or Competition: Hackers may target web3 companies in African countries to inflict reputation damage on competitors or gain a competitive advantage. Breaching a competitor's platform and exposing vulnerabilities or compromising customer trust can create a negative perception that benefits other players in the market.

f. Limited Regulatory Frameworks: In some cases, hackers exploit gaps or weaknesses in regulatory frameworks governing web3 companies in African countries. Insufficient regulations or enforcement may embolden cybercriminals and make it easier for them to operate without significant consequences.

g. Technical Skills Showcase: Hacking web3 companies can be seen as a way for individuals or groups to demonstrate their technical skills or establish a reputation within the hacking community. This motivation may be driven by personal satisfaction, peer recognition, or a desire to be part of a cybercriminal network.

It is important to note that motivations can vary significantly among hackers, and the actual motivations behind specific breaches in African web3 companies may not fit neatly into these categories. Each case requires thorough investigation to uncover the precise motives behind the attacks.

The breaches at Patricia and Flutterwave underscore the importance of prioritizing cybersecurity in web3 companies operating in Africa. Comparative analysis revealed that breaches in web3 companies are not limited to Africa but occur globally. To mitigate risks, companies must invest in robust security measures, conduct regular audits, enhance employee training, and collaborate with relevant stakeholders. By adopting a proactive approach to security, web3 companies can better protect their platforms, users, and assets, fostering trust and promoting the growth of the web3 ecosystem in Africa and beyond.

REFERENCE:

Abiodun, "Patricia to temporarily suspend withdrawals after security breach," 26 03 2023.
https://techpoint.africa/2023/05/26/patricia-suffers-security-breach/

Abiodun, "Hackers steal 2.9 billion from Flutterwave accounts, motion granted to freeze accounts connected with stolen funds," 05 05 2023. [Online].
https://techpoint.africa/2023/03/05/hackers-have-stolen-2-9-billion-from-flutterwave/https://rpajournals.com/wp-content/uploads/2022/05/JIBM-2022-04-5373.pdf
https://www.cio.com/article/220241/how-8-middle-eastern-countries-are-jump-starting-blockchain-development.html
https://www.bakermckenzie.com/-/media/files/insight/publications/2019/02/report_blockchainandcryptocurrencyreg_feb2019.pdf

Africa Blockchain Institute 3rd Edition Report
Crypto-Oasis-Ecosystem-Report-2023-Spring-Edition
CV VC Africa Blockchain Report
https://emurgo.io/adaverse-accelerator-launches-start-up-school/https://techcabal.com/2023/03/10/echovc-launches-8-million-fund-for-blockchain-powered-startups/

V.
Beosin Security Services and Products

Beosin Security Product

Beosin EagleEye

Security monitoring, alerting and blocking

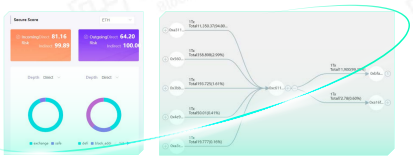
Based on AI technology, combined with on-chain and off-chain real-time data analysis, and open source intelligence, it can timely discover security risks, send alerts and block risk transactions during the operation of Web 3.0 projects. Subscribers will receive real-time warnings for 10 kinds of abnormal risk transactions such as large transfers, flashloans, privilege changes, price drops, etc. It plays a role in hacking, fraud, rug pull and other security issues prevention. Now more than 2,300 Web 3.0 projects have been monitored by Beosin EagleEye.

Try Beosin EagleEye: https://eagleeye.beosin.com/

Add Beosin Alert to your browser to detect phishing sites:
https://chrome.google.com/webstore/detail/beosin-alert/lgbhcpagiobjacpmcgckfgodjeogceji?hl=en

Beosin KYT

AML and crypto compliance platform

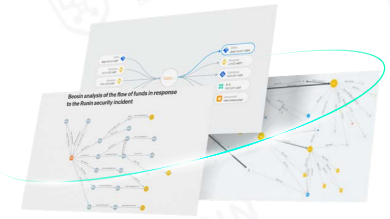


Relying on more than 1 billion address tags and malicious address database, Beosin KYT, the cryptocurrency AML and crypto compliance platform can help VASP (Virtual Asset Service Providers) build KYT (Know Your Transactions) and risk assessment capabilities. The system analyzes massive amounts of on-chain transactions to identify transactions and address types, and then uses the system's massive library of entity addresses and machine learning analytics to assess risky transactions. Beosin KYT are currently serving multiple clients around the world to comply with AML regulations.

Try Beosin KYT: https://kyt.beosin.com/

Beosin Trace

Cryptocurrency tracing and investigation platform



Beosin-Trace is a cryptocurrency fund tracing platform that combines big data, AI and other technologies. It is a personalized investigation tool for global clients in recovering their lost cryptocurrencies. It has successfully helped clients recover 100+ millions of stolen assets, including funds that flowed into mixers (such as Tornado Cash).

Try Beosin Trace: https://beosin.com/service/tracing

Beosin VaaS

Formal verification platform for smart contracts

Beosin security team uses multiple technologies such as formal verification and fuzzy testing as core technologies to develop VaaS, a highly automated security detection tool for smart contracts, with an accuracy of 97% and can automatically detect hundreds of security vulnerabilities of smart contracts in one-click.

Try Beosin VaaS: https://vaas.beosin.com/

About Blockchain Security Alliance

The Blockchain Security Alliance was initiated by Beosin in joint collaboration with several units from diverse industry backgrounds, including university institutions, blockchain security companies, industry associations, fintech service providers, etc. The first batch of alliance council include Beosin, SUSS NiFT, NUS AIDF, BAS, FOMO Pay, Onchain Custodian, Semisand, Coinhako, ParityBit, and Huawei Cloud. The current members include: Huobi University, Moledao, Least Authority, PlanckX, Coding Girls, Coinlive, Footprint Analytics, Web3Drive, and Digital Treasures Center. The members of the Security Alliance will work and cooperate together to continuously secure the global blockchain ecosystem with their own technical strengths. The Alliance Council also welcomes more people in blockchain-related fields to join and jointly defend the security of the blockchain ecosystem.

Alliance Registration： https://forms.gle/pb3NaUgS3a2Sswnc8

Contact： @kristenbeosin @Web3Donny market@beosin.com

About Beosin

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, UAE, Korea, Japan and other 10+ countries. With the mission of "Securing Blockchain Ecosystem", Beosin provides "All-in-One" blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 3000 smart contracts including famous Web3 projects PancakeSwap, Uniswap, DAI, OKSwap and all of them are monitored by Beosin EagleEye. The KYT AML are serving 100+ institutions including Binance.

About SUSS NiFT

The SUSS Node for Inclusive Fintech (NiFT) is the "Centre of Excellence" spearheading all Fintech initiatives at the university. It is a multi-disciplinary centre drawing on expertise from faculty members across SUSS' five schools, their collective publications and programmes. Established in 2021, SUSS NiFT is essentially a re-launch of SUSS' endeavor in the Fintech and blockchain domain since 2016. NiFT serves to deliver high-quality research, public education, and policy advocacy for inclusivity in the Financial Technology sector for the benefit of society.

About LegalDAO

LegalDAO is a decentralized community that gathers global Web3 legal professionals and enthusiastic participants, dedicated to building a global Web3 legal ecosystem. Through initiating the bottom-up "2023 Crypto Consensus Referendum," establishing a social relationship-based on-chain identity system "De-X," a decentralized self-governance system "De-Reg," and Web3 legal research, education, socialization, and other content, we call on everyone to work together to complete the great practice of establishing Web3 native order.

About Footprint Analytics

Footprint Analytics is a data platform blending web2 and web3 data with abstractions. We help analysts, builders, and investors turn blockchain data into insights with accessible visualization tools and a powerful multi-chain API across 20+ chains for NFTs, GameFi and DeFi. We also provide Footprint Growth Analytics to help with effective growth in GameFi and any web3 projects.

About Biteye

Biteye is Asia's leading Web3 research community, generating forward-looking investment research content and tools through community and AI-driven approaches, helping community members explore the Web3 rabbit hole.

About ShellBoxes

ShellBoxes is a leading Web3 firm focused on providing top-notch blockchain security solutions & development services for decentralized applications (dApps) on Ethereum and Solana. Our team of experts specializes in smart contracts development, auditing, testing, and implementation of advanced security strategies. We prioritize user privacy and aim to make decentralized technology more accessible and trustworthy for businesses and individuals.

CONTACT US

market@beosin.com
Email

t.me/beosin
Telegram

@Beosin_com
Official Twitter

@BeosinAlert
Alert Twitter